WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Monday, April 10, 2006

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=OR	
☐	L117	380/201.ccls. and (bore near4 resist$5)	1
☐	L116	l108 and (bore near3 resist$4)	5
☐	L115	(JAKUBOWSKI near2 MARIUSZ) and (oblivious$3)	2
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L114	(insert$7 and extra and instruction$2 and input$3 and (checksum or hash$4 or CRC)).clm.	2
☐	L113	(insert$7 and instruction$2 and input$3 and (checksum or hash$4 or CRC)).clm.	63
☐	L112	(insert$7 and instruction$2 and unput$3 and chacksum).clm.	0
☐	L111	L110 and (input near4 (function$3 or segment$7 or content$4))	25
☐	L110	L109 and (cheksum or hash$3 or CRC)	81
☐	L109	(713/167 |713/176 |713/187 |713/179 |713/190 |713/201).ccls. and ((software or content$2) same (protect$7 or prevent$7)same run$3)	152
☐	L108	(713/167 |713/176 |713/187 |713/179 |713/190 |713/201).ccls. and (software nea4 tamp$7 nea4 resst$7)	2000
☐	L107	(l104 or l103 or l102 or l101) and (input near4 checksum)	1
☐	L106	(l104 or l103 or l102 or l101) and (oblivious$7)	2
☐	L105	(l104 or l103 or l102 or l101) and ((obfuscat$7) and (checksum or hash$4 or CRC))	3
☐	L104	(6801999 6895503 6898706 6816596 6885748 6697944).pn.	12
☐	L103	(6240183|6263313|6636530|6782478).pn.	8
☐	L102	(5933501|5980080|6041316).pn.	6
☐	L101	(5745569|5768372|5812671|5852664|5915017).pn.	10
☐	L100	(5745569|5768372|5812671|5852664|5915017).pn	151
☐	L99	("5159630"|"5199069"|"5365589"|"5548648"|"5742686").pn	106
☐	L98	(726/2).ccls. and (obfuscat$7) and (checksum or hash$4 or CRC)	2
☐	L97	(726/2).ccls. and (obfuscat$7)	6
☐	L96	(726/2).ccls. and (checksum near5 embed$7)	0
☐	L95	(726/2).ccls. and (software adj protection)	4
☐	L89	L88 and oblivious adj check$9	0
☐	L88	(705/50 |705/57 |705/58 |705/59).ccls.	1557
☐	L87	wo adj3 9704394 and signature	0
☐	L86	wo adj3 9704394 and (hash)	0
☐	L85	wo adj3 9704394 and (checksum)	0

☐	L84	wo adj3 9704394	2
☐	L83	6782478	3
☐	L82	6782478 and (signature)	2
☐	L81	6782478 and (checksum or hash$2 or parity$3)	2
☐	L80	5613004.pn. and (checksum or hash$4 or parity)	1
☐	L79	5613004.pn. and (checksum)	0
☐	L78	L77 and register	77
☐	L77	L76 and encrypt$4	96
☐	L76	L75 and stega$8	102
☐	L75	5319735 and (checksum or hash$2 or CRC or parity)and software	147
☐	L74	5319735 and (checksum or hash$2 or CRC or parity)and software	147
☐	L73	5319735.pn. and (checksum or hash$2 or CRC or parity)	0
☐	L72	5319735.pn. and (checksum or hash$2 or CRC or parity)	0
☐	L71	5319735.pn. and (checsum or hash$2 or CRC or parity)	0
☐	L70	5319735.pn. and (checsum or hash$2 or CRC or prity)	0
☐	L69	5319735 and (checsum or hash)	103
☐	L68	(5530752| 5649099| 5745569| 5748741)![pn] and hash	1
☐	L67	(5530752| 5649099| 5745569| 5748741)![pn] and checksum	0
☐	L66	(5530752| 5649099| 5745569| 5748741)![pn]	8
☐	L65	6,782,478.pn.	2
☐	L64	checksum same function same modification same register	11
☐	L63	checksum near10 function same modification same register	1
☐	L61	multiple adj input adj shift near4 register and checksum and software	2
☐	L60	multiple adj input adj shift near4 register same checksum and software	1
☐	L59	multiple adj input adj shift near4 register same checksum same software	0
☐	L58	multiple adj input adj shift near4 register near6 checksum	1
☐	L57	5054787.pn.	2
☐	L56	6256777.pn.	2
☐	L55	5379345.pn.	2
☐	L54	5379345.pn. and (checksum or hash$4)	0
☐	L53	5379345.pn. and (checksum or hash$4)	0
☐	L52	5745569.pn. and (checksum or hash$4)	1
☐	L51	6782478.pn. and checksum	1
☐	L50	modifying adj3 (memory or register) same checksum	7
☐	L49	paging adj (subsyetem or sub adj system) and (checksum or integrity)	6
☐	L48	paging adj subsyetem and (checksum or integrity)	0
☐	L47	paging adj subsyetem and checksum	0

DB=USPT; PLUR=YES; OP=OR

☐	L44	(L43 or L38)and digital adj content or siftware	73
☐	L43	(380/201).ccls.	380
☐	L42	(380/50).ccls.	0
☐	L41	L40 and software adj protection	5
☐	L40	(713/191 |380/43 |380/49).ccls.	372
☐	L39	L38 and register and checksum	25
☐	L38	(713/187).ccls.	180
☐	L37	L36 and obli$8	6
☐	L36	VENKATESAN.in.	272
☐	L34	L32 and register	0
☐	L33	L32 and memory	1
☐	L32	5852664.pn.	1
☐	L31	6,643,821.pn.	1
☐	L30	5386469 and checksum	6
☐	L29	5386469 and checsum	0
☐	L28	5386469.pn.	1
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L27	L26 and integrity	7
☐	L26	arani and pag$7	61
☐	L25	L24 and checksum	0
☐	L24	debug$6 and breakpont$7	1
☐	L23	debug$6 and bearkpont$7	0
☐	L22	debug$6 and (braekpoint$7 same checksum)	0
☐	L21	debug$6 same braekpoint$7	0
☐	L20	debug$6 same braekpoint	0
☐	L19	debug$6 same braekpoint and checksum	0
☐	L18	debug$6 same braekpoint same checksum	0
		DB=USPT; PLUR=YES; OP=OR	
☐	L17	US-6256777-B1.did.	1
		DB=USPT,PGPB,JPAB,EPAB; PLUR=YES; OP=OR	
☐	L16	(US-6256777-B1)![pn]	0
☐	L15	(US-6256777-B1)![pn]	0
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L14	6256777	5
☐	L13	6256777 and encrypt$4	0
☐	L12	6256777 and parity	0
☐	L11	6256777 and crc	0
☐	L10	6256777 and checksum	0

☐	L9	debug$7 near4 checksum	14
☐	L8	L7 near5 modif$7	4
☐	L7	checksum near5 register	451
☐	L6	20050210275	2
☐	L5	09/525694	3
☐	L4	5892899 and (hash or checksum) and (insert$6 or inject$7)	13
☐	L3	5892899 and (hash or checksum)	24
☐	L2	5892899.pn. and (hash or checksum)	0
☐	L1	5892899.pn.	2

END OF SEARCH HISTORY

STIC Search Report
4/10/2006

EIC 2100

SN. 09651901

```
Set     Items   Description
S1    3368926   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
           AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2    2670176   INSTRUCTION? ? OR OPERATION? ? OR CODE OR CODING OR CERTIF-
           ICATE? ? OR SIGNATURE? ? OR WATERMARK? ? OR WATER()MARK? ?
S3      40843   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
            OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
           EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)S2
S4      18763   (ADD OR ADDS OR ADDED OR ADDING)(5N)S2
S5    1897014   MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHAN-
           GE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATIO-
           NS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?
S6      13804   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
            HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
           UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
           OR MESSAGE()AUTHENTICATION()CODE
S7       2651   (S3 OR S4) AND S1 AND S5
S8        778   ((S3 OR S4) (10N) S1) AND S5
S9         42   S7 AND S6
S10        18   S9 AND IC=G06F
S11        18   IDPAT (sorted in duplicate/non-duplicate order)
S12        18   IDPAT (primary/non-duplicate records only)
S13   4406137   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
           OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
           PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
           E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?
           ? OR IMAGE?
S14   6062253   DATA OR FILE OR CONTENT? ? OR S13
S15    183764   S5 (5N)S14
S16       457   S3 AND S1 AND S15
S17       233   S16 AND S13
S18       120   (S3 (10N) S1) AND S15
S19        63   S18 AND S13
S20        18   S19 AND AY=1963:2000
S21        18   IDPAT (sorted in duplicate/non-duplicate order)
S22        18   IDPAT (primary/non-duplicate records only)
S23        18   S22 NOT S12
S24        16   S19 AND PY=1976:2000
S25         7   S24 NOT (S12 OR S23)
S26         7   IDPAT (sorted in duplicate/non-duplicate order)
S27         7   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
        (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200622
        (c) 2006  Thomson Derwent
```

27/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06579861 **Image available**
DATA OUTPUT CONTROLLER, DATA PROCESSOR AND STORAGE MEDIUM READ BY COMPUTER

PUB. NO.: 2000-165652 [JP 2000165652 A]
PUBLISHED: June 16, 2000 (**20000616)**
INVENTOR(s): YOSHIDA ATSUSHI
IWAMURA KEIICHI
APPLICANT(s): CANON INC
APPL. NO.: 10-337259 [JP 98337259]
FILED: November 27, 1998 (19981127)
INTL CLASS: H04N-001/387; G06F-003/12; G09C-005/00

ABSTRACT

PROBLEM TO BE SOLVED: To protect copyright of digital contents by properly controlling print data in the case of printing out the digital contents with a digital watermark imbedded by a printer.

SOLUTION: A digital watermark extract section 106 uses digital **watermark imbedded** position information to extract **imbedded** information from **picture** data generated by an **application software** 102. Then a **picture modification** section 108 applies **modification** processing to add imbedded information (e.g. density correction data) to a density of a **picture** so as to **modify** the **picture** . The **picture data** that receives **picture modification** processing are given to a print data generating section 109 together with print control information such as a size of paper on which the **picture** data are printed to generate print data, which can be printed by a printer 112. A **picture** transfer section 110 transfers the generated print data to the printer 112, where the print data are printed out.

27/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

02746907 **Image available**
OUTPUT SYSTEM FOR PMC LADDER **GRAPHIC**

PUB. NO.: 01-044507 [JP 1044507 A]
PUBLISHED: February 16, 1989 (**19890216)**
INVENTOR(s): NAKAJIMA SACHIHIRO
HOSHINO YOSHINORI
APPLICANT(s): FANUC LTD [419041] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 62-201595 [JP 87201595]
FILED: August 12, 1987 (19870812)
INTL CLASS: [4] G05B-019/04; G06F-009/06
JAPIO CLASS: 22.3 (MACHINERY -- Control & Regulation); 45.1 (INFORMATION PROCESSING -- Arithmetic Sequence Units)
JOURNAL: Section: P, Section No. 880, Vol. 13, No. 242, Pg. 32, June 07, 1989 (19890607)

ABSTRACT

PURPOSE: To print out only a changed page by forming a print instruction to be neglected at the time of executing a ladder program and validated only in case of printing-out operation.

CONSTITUTION: When a dummy page inserting instruction 1 is executed, a ladder is added to a dummy page 4 specified based on the number 2 of dummy pages. When such kind of dummy page **inserting instructions** are **inserted** into respective **function** blocks in a ladder **graphic** , a **changed** part may be added to a dummy page and only the changed part can be printed out.

23/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014687563 **Image available**
WPI Acc No: 2002-508267/200254
XRPX Acc No: N02-402249

Embedding watermark in information signal by determining local weight factors from spatial, motion, scene change and human visual system properties

Patent Assignee: KONINK PHILIPS ELECTRONICS NV (PHIG)
Inventor: DEPOVERE G F G; HAITSMA J A; KALKER A A C M
Number of Countries: 024 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200239383	A2	20020516	WO 2001EP12588	A	20011029	200254 B
US 20020087864	A1	20020704	US 20013066	A	20011102	200254
KR 2002071927	A	20020913	KR 2002708799	A	20020706	200311
CN 1411590	A	20030416	CN 2001806071	A	20011029	200345
EP 1336160	A2	20030820	EP 2001991716	A	20011029	200362
			WO 2001EP12588	A	20011029	
JP 2004513586	W	20040430	WO 2001EP12588	A	20011029	200430
			JP 2002541627	A	20011029	

Priority Applications (No Type Date): EP 2000203893 A 20001107
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200239383	A2	E	15	G06T-001/00	
Designated States (National): CN JP KR					
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR					
US 20020087864	A1			H04L-009/00	
KR 2002071927	A			H04N-005/913	
CN 1411590	A			G06T-001/00	
EP 1336160	A2	E		G06T-001/00	Based on patent WO 200239383
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR					
JP 2004513586	W		30	H04N-007/08	Based on patent WO 200239383

Abstract (Basic): WO 200239383 A2

NOVELTY - Method consists in determining local weight factors based on temporal and spatial **data** , motion **data** , motion estimation, scene **changes** and human visual system properties to make the watermark imperceptible when embedded in the information signal.

DETAILED DESCRIPTION - There are INDEPENDENT CLAIMS for (1) a system for **embedding** a **watermark** in an information signal, (2) a watermarking **program** .

USE - Method is for embedding a watermark in an information signal e.g. an **MPEG** **video** signal.

DESCRIPTION OF DRAWING(S) - The figure shows a watermark embedding system.

pp; 15 DwgNo 1/2

Title Terms: EMBED; WATERMARK; INFORMATION; SIGNAL; DETERMINE; LOCAL; WEIGHT; FACTOR; SPACE; MOTION; SCENE; CHANGE; HUMAN; VISUAL; SYSTEM; PROPERTIES
Derwent Class: T01; W04
International Patent Class (Main): G06T-001/00; H04L-009/00; H04N-005/913; H04N-007/08
International Patent Class (Additional): G06T-007/20; H04N-001/387; H04N-007/081
File Segment: EPI

23/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014533104 **Image available**
WPI Acc No: 2002-353807/200239
XRPX Acc No: N02-278007
Digital watermark data embedding method for still pictures **, involves** changing **feature value of portion of** content **data based on embedding strength map**
Patent Assignee: HITACHI LTD (HITA); HITACHI SEISAKUSHO KK (HITA); ECHIZEN I (ECHI-I); EIKAWA S (EIKA-I); HARANO S (HARA-I); SASAKI R (SASA-I); YOSHIURA H (YOSH-I)
Inventor: ECHIZEN I; EIKAWA S; HARANO S; SASAKI R; YOSHIURA H
Number of Countries: 030 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1170938	A2	20020109	EP 2001105611	A	20010306	200239	B
CN 1333627	A	20020130	CN 2001117314	A	20010228	200239	
JP 2002027225	A	20020125	JP 2000205512	A	20000706	200239	
US 20020007403	A1	20020117	US 2001798928	A	20010306	200239	
KR 2002005376	A	20020117	KR 20019503	A	20010224	200250	
KR 409164	B	20031218	KR 20019503	A	20010224	200425	

Priority Applications (No Type Date): JP 2000205512 A 20000706
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1170938	A2	E	18	H04N-001/32	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
CN 1333627	A			H04N-005/262	
JP 2002027225	A		13	H04N-001/387	
US 20020007403	A1			G06F-015/16	
KR 2002005376	A			G06T-009/00	
KR 409164	B			G06T-009/00	Previous Publ. patent KR 2002005376

Abstract (Basic): EP 1170938 A2
NOVELTY - An embedding strength map indicating change being allowed for feature value of a portion of content data for embedding watermark data, is stored in a database (152). Digital watermark data is embedded in the **content data** , by **changing** the feature value of the **content** portion based on the indication in the map.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) Digital watermark embeddability analyzing method;
(b) Digital watermark embedding apparatus;
(c) Digital watermark embeddability analyzing apparatus;
(d) Recorded medium storing digital **watermark** data **embedding program**
USE - For embedding digital watermark data in content data such as still **images** , moving **picture images** for copyright protection.
ADVANTAGE - The load of embeddability analyzing process and embedding process in content data are greatly reduced, and hence processing is faster leading to greater efficiency.
DESCRIPTION OF DRAWING(S) - The figure shows the schematic view of content distribution center.
Database (152)
pp; 18 DwgNo 2/7
Title Terms: DIGITAL; WATERMARK; DATA; EMBED; METHOD; STILL; **PICTURE** ; CHANGE; FEATURE; VALUE; PORTION; CONTENT; DATA; BASED; EMBED; STRENGTH; MAP
Derwent Class: T01; W02; W04
International Patent Class (Main): G06F-015/16; G06T-009/00; H04N-001/32; H04N-001/387; H04N-005/262

International Patent Class (Additional): G06T-001/00; H04N-005/272;
H04N-007/08; H04N-007/081; H04N-007/173
File Segment: EPI

23/5/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014431655 **Image available**
WPI Acc No: 2002-252358/200230
Personal information management service method using code image **physically represented and apparatus thereof**
Patent Assignee: COLOURZIP MEDIA CO LTD (COLO-N); COLORZIP MEDIA INC (COLO-N)
Inventor: HAN T D; JUNG C H; LEE N G; SHIN E D; CHUNG C H
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2001100716	A	20011114	KR 200024203	A	20000506	200230	B
JP 2003006200	A	20030110	JP 2001171467	A	20010606	200315	N
KR 421247	B	20040304	KR 200024203	A	20000506	200444	

Priority Applications (No Type Date): KR 200024203 A 20000506; JP 2001171467 A 20010606
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2001100716	A		1	G06F-017/40	
JP 2003006200	A		18	G06F-017/30	
KR 421247	B			G06F-017/40	Previous Publ. patent KR 2001100716

Abstract (Basic): KR 2001100716 A
NOVELTY - A personal information management service method using code **images** physically represented and an apparatus thereof are provided to add or **change** or erase **contents** of a database by using personal information converted to code **images** .
DETAILED DESCRIPTION - A server computer(12) is connected with a transmitter computer(15)and a recipient computer(18) by a communication network(11). The server computer(12) provides an encoding software(12c) and a decoding software(12d) to users and includes a global database(12a) for storing personal information of all users and a user database(12b) for storing information of persons managed by each user. The encoding software(12c,15c) and the decoding software(12d,18d) encode and decode personal information according to a predetermined method. The transmitter computer(15) stores the personal information in the global database(12a), encodes the personal information to code **images** (16a) by using the encoding **software** (15c), **inserts** the **code images** into a personal information medium(16), and transmits the personal information medium(16) to the recipient computer(18). A data converter(17) receives and converts the code **images** from the transmitter computer(15). The recipient computer(18) decodes the converted code data by using the decoding software(18d), extracts the personal information from the decoded code **images** , and stores and manages the extracted personal information.
pp; 1 DwgNo 1/10
Title Terms: PERSON; INFORMATION; MANAGEMENT; SERVICE; METHOD; CODE; **IMAGE** ; PHYSICAL; REPRESENT; APPARATUS
Derwent Class: T01
International Patent Class (Main): G06F-017/30; G06F-017/40
File Segment: EPI

23/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013979256 **Image available**
WPI Acc No: 2001-463470/200150
XRPX Acc No: N01-343565

Integrated information browsing method over internet, involves registering persistency control configured to selectively prevent attempts to replace data within browser

Patent Assignee: INTEL CORP (ITLC)
Inventor: KUKKAL P
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6182073	B1	20010130	US 97859055	A	19970520	200150	B

Priority Applications (No Type Date): US 97859055 A 19970520
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6182073	B1		18	G06F-017/30	

Abstract (Basic): US 6182073 B1

NOVELTY - Multiple-participant application is executed and persistency control which monitors and selectively prevents attempts to replace data within information browser, is registered. Output of multiple-participant **application** is embedded in a portion of information browser window. **Embedding operation** is non-responsive to attempts to replace data until persistency is disabled and persists per persistency control.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Article of manufacture;
(b) Information browsing apparatus;
(c) Computer readable medium;
(d) Information browsing system

USE - For browsing information on internet and executing application such as **video** conferencing application.

ADVANTAGE - Allows user to **modify** the control options of **video** conferencing through web pages by displaying them. Enables seemless integration of information browsing from multiple independent uncollaborated information sources.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart illustrating the steps of multiple participant application method.

pp; 18 DwgNo 3B/8

Title Terms: INTEGRATE; INFORMATION; METHOD; REGISTER; CONTROL; CONFIGURATION; SELECT; PREVENT; ATTEMPT; REPLACE; DATA
Derwent Class: T01; W01; W02
International Patent Class (Main): G06F-017/30
File Segment: EPI

23/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013840057 **Image available**
WPI Acc No: 2001-324270/200134
Related WPI Acc No: 2002-743444
XRPX Acc No: N01-233837
Electronic camera with electronic watermark embedding function **, has central processing unit which controls** recording **of electronic** image **data with and without embedded electronic watermark in memory**
Patent Assignee: NIKON CORP (NIKR); NIKON GIJUTSU KOBO KK (NIKR); NIKON TECHNOLOGIES INC (NIKR)
Inventor: OHMURA A
Number of Countries: 002 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 2001086449	A	20010330	JP 99256548	A	19990910	200134 B
US 6963363	B1	20051108	US 2000655917	A	20000906	200573
US 20050280723	A1	20051222	US 2000655917	A	20000906	200603
			US 2005199149	A	20050809	

Priority Applications (No Type Date): JP 99256548 A 19990910; JP 2000105973 A 20000407
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001086449	A		11	H04N-005/91	
US 6963363	B1			H04N-005/76	
US 20050280723	A1			H04N-005/228	Div ex application US 2000655917 Div ex patent US 6963363

Abstract (Basic): JP 2001086449 A
NOVELTY - A watermark implanting circuit (204) embeds electronic watermark to electronic **image** data of the photographed object of an **image** pick-up circuit (202). A **recording** circuit (206) stores electronic **image** data in a memory (207). A central processing unit (CPU) (201) controls the **recording** of **image** data with and without electronic watermark in the memory.
USE - Electronic camera.
ADVANTAGE - Offers electronic camera with copyright protection and **alteration** prevention function and prevents **image data** quality degradation.
DESCRIPTION OF DRAWING(S) - The figure shows a block diagram for explaining the function of an electronic camera.
CPU (201)
Image pick-up circuit (202)
Watermark implanting circuit (204)
Recording circuit (206)
Memory (207)
pp; 11 DwgNo 2/4
Title Terms: ELECTRONIC; CAMERA; ELECTRONIC; WATERMARK; EMBED; FUNCTION; CENTRAL; PROCESS; UNIT; CONTROL; RECORD; ELECTRONIC; **IMAGE** ; DATA; EMBED ; ELECTRONIC; WATERMARK; MEMORY
Derwent Class: T01; W02; W04
International Patent Class (Main): H04N-005/228; H04N-005/76; H04N-005/91
International Patent Class (Additional): G06K-009/00; G06K-009/36; H04N-001/387; H04N-005/225; H04N-007/00; H04N-011/00
File Segment: EPI

23/5/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013779166 **Image available**
WPI Acc No: 2001-263377/200127
XRPX Acc No: N01-188731
Recording **device** modifies **non-** recording **indication when other broadcast program is chosen during non-** recording **condition of one broadcast program**
Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU); MATSUSHITA ELECTRIC IND CO LTD (MATU)
Inventor: ISHIHARA H; MITSUI Y; NAGAI T
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2001054061	A	20010223	JP 2000160995	A	20000530	200127	B
US 6802074	B1	20041005	US 2000584145	A	20000531	200465	

Priority Applications (No Type Date): JP 99151658 A 19990531
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2001054061	A		18	H04N-005/91	
US 6802074	B1			H04N-007/16	

Abstract (Basic): JP 2001054061 A
NOVELTY - A reading unit (8) reads electronic water mark embedded in received **video** area. An indication unit indicates **recording** unit to record successive **video** area when **recording** approval purport is shown in read water mark and to stop **recording** when **recording** prohibition purport is shown. During non- **recording** condition, if other broadcast program is chosen, non- **recording** indication is modified by **modifying** unit.
DETAILED DESCRIPTION - Receiver receives **video** area which comprises selected broadcast program. INDEPENDENT CLAIMS are also included for the following:
(a) Transmission device;
(b) **Recording** medium
USE - To record received broadcast program on **recording** medium.
ADVANTAGE - Records latter broadcast program on **recording** medium without missing, even when two broadcast **programs** where copy control information is **embedded** as an electronic **water mark** is received continuously.
DESCRIPTION OF DRAWING(S) - The figure shows the components of **recording** device.
Reading unit (8)
pp; 18 DwgNo 5/15
Title Terms: RECORD; DEVICE; MODIFIED; NON; RECORD; INDICATE; BROADCAST; PROGRAM; CHOICE; NON; RECORD; CONDITION; ONE; BROADCAST; PROGRAM
Derwent Class: W04
International Patent Class (Main): H04N-005/91; H04N-007/16
International Patent Class (Additional): H04N-005/44; H04N-005/765; H04N-005/92; H04N-007/08; H04N-007/081
File Segment: EPI

23/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013431602 **Image available**
WPI Acc No: 2000-603545/200058
XRPX Acc No: N00-446652

Watermark embedding method for embedding watermark in digital image such that watermark is imperceptible visually digital data, in which watermark is embedded into digital content such that it cannot be perceived by person

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE)
Inventor: NAKAMURA T; OGAWA H; TAKASHIMA Y; TOMIOKA A
Number of Countries: 026 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1022678	A2	20000726	EP 99309199	A	19991118	200058	B
JP 2000287073	A	20001013	JP 99303185	A	19991025	200101	
JP 2003078756	A	20030314	JP 99303185	A	19991025	200328	
			JP 2002144947	A	19991025		
JP 2003219148	A	20030731	JP 99303185	A	19991025	200351	
			JP 2002333324	A	19991025		
JP 3654263	B2	20050602	JP 99303185	A	19991025	200537	
			JP 2002144947	A	20020520		
JP 3745729	B2	20060215	JP 99303185	A	19991025	200617	
			JP 2002333324	A	20021118		

Priority Applications (No Type Date): JP 9916219 A 19990125; JP 9916218 A 19990125
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1022678	A2	E	210	G06T-001/00	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
JP 2000287073	A		117	H04N-001/387	
JP 2003078756	A		37	H04N-001/387	Div ex application JP 99303185
JP 2003219148	A		101	H04N-001/387	Div ex application JP 99303185
JP 3654263	B2		35	H04N-001/387	Div ex application JP 99303185 Previous Publ. patent JP 2003078756
JP 3745729	B2		117	H04N-001/387	Div ex application JP 99303185 Previous Publ. patent JP 2003219148

Abstract (Basic): EP 1022678 A2

NOVELTY - The watermark embedding and detection method is provided to actualize copyright protection for digital **content** , **change** personal information **content** by a small amount that cannot be perceived, and embed watermark such that it cannot be perceived by a person into the content.

DETAILED DESCRIPTION - The watermark embedding method involves embedding a watermark into a digital **image** such that it is imperceptible visually digital **data** . The method involves **changing** independently a real number component and an imaginary number component of each of coefficient values of a complex watermark coefficient matrix using a key, and the watermark to be embedded in the digital **image** . A watermark pattern is generated by performing a discrete Fourier transform on the **changed** watermark coefficient matrix. An embedded **image** is generated by adding like tiling the watermark pattern to the digital **image** . INDEPENDENT CLAIMS are included for; a watermark embedding apparatus that embeds a watermark into a digital **image** such that it is imperceptible; a watermark detection apparatus for detecting a watermark in a detected object **image** ; a storage medium that stores a **watermark embedding program** that performs **embedding** of a **watermark** ; a storage medium that stores a watermark detection **program** ; a **watermark** system that **embeds watermark** into a digital **image**

USE - Embedding a watermark that cannot be sensed by a person, into digital data

ADVANTAGE - Provides adaptive information embedding for visual characteristics to high degree, and increases relative robustness of he watermark.

DESCRIPTION OF DRAWING(S) - The drawing shows a diagram of the configuration of a watermark embedding apparatus according to the invention.

Watermark embedding apparatus (100)
Input **image** (101)
Intensity parameter (102)
Watermark (103)
Key (104)
Embedded **image** (105)
pp; 210 DwgNo 1/138

Title Terms: WATERMARK; EMBED; METHOD; EMBED; WATERMARK; DIGITAL; **IMAGE** ; WATERMARK; VISUAL; DIGITAL; DATA; WATERMARK; EMBED; DIGITAL; CONTENT; PERCEPTION; PERSON

Derwent Class: P85; T01; W02; W04

International Patent Class (Main): G06T-001/00; H04N-001/387

International Patent Class (Additional): G09C-005/00; H04N-007/08; H04N-007/081

File Segment: EPI; EngPI

23/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012347048 **Image available**
WPI Acc No: 1999-153155/199913
Related WPI Acc No: 1998-008272
XRPX Acc No: N99-110428
Data embedding method in still image **for** image **encoder in stenography field**
Patent Assignee: MASSACHUSETTS INST TECHNOLOGY (MASI)
Inventor: BENDER W; GRUHL D; MORIMOTO N
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5870499	A	19990209	US 96599254	A	19960209	199913	B
			US 97971586	A	19971117		

Priority Applications (No Type Date): US 96599254 A 19960209; US 97971586 A 19971117
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5870499	A		14	G06K-009/36	Cont of application US 96599254 Cont of patent US 5689587

Abstract (Basic): US 5870499 A

NOVELTY - The **image** is **altered** by increasing the parameter value of at least some first points and first patch of points surrounding each first point. The parameter value of at least some second points and second patch of points surrounding each second point is decreased.

DETAILED DESCRIPTION - An ordered services of pseudo- random numbers are generated, and each one is assigned to a first or second group. Each pseudo-random number is associated with a point. Each point associated with pseudo-random number assigned to the first group is designated as first point, and that of to second group is designated as second point. INDEPENDENT CLAIMS are included for the following:

(a) data embedding apparatus in **image** ;

(b) determination apparatus of whether text **image** is electronically encoded as points;

(c) **image** created by **altering** host **image** .

USE - For hiding data pattern in host **image** for **image** encoder in stenography field.

ADVANTAGE - Ensures low-bit-rate data **embedding** such as signature marking of digitally represented **images** . **Application** of **changes** to patches protects the embedded bit from obliteration by lossy compression, tone correction, filtering, cropping and affine transformation.

DESCRIPTION OF DRAWING(S) - The figure shows flow chart illustrating encoding process.

pp; 14 DwgNo 6/7

Title Terms: DATA; EMBED; METHOD; STILL; **IMAGE** ; **IMAGE** ; ENCODE; FIELD
Derwent Class: T01
International Patent Class (Main): G06K-009/36
File Segment: EPI

23/5/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012022804 **Image available**
WPI Acc No: 1998-439714/199838
XRPX Acc No: N98-342695

Watermark-embedding-extracting of identification information into-from picture **data - generating combinations of basis functions orthogonal each other for each numerical signal, and for each combination, calculating corresponding weight coefficient by using sum of products of basis** functions for pixels in original picture

Patent Assignee: FUJITSU LTD (FUIT)
Inventor: KAZUI K; MORIMATSU E; NAKAGAWA A; TADA A; TANAKA K
Number of Countries: 025 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 860984	A2	19980826	EP 97117824	A	19971015	199838 B
JP 10234012	A	19980902	JP 9735258	A	19970219	199845
US 6104826	A	20000815	US 97948083	A	19971009	200041
EP 860984	B1	20040114	EP 97117824	A	19971015	200406
DE 69727206	E	20040219	DE 97627206	A	19971015	200419
			EP 97117824	A	19971015	
JP 3686741	B2	20050824	JP 9735258	A	19970219	200556

Priority Applications (No Type Date): JP 9735258 A 19970219
Cited Patents: No-SR.Pub
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 860984	A2	E	26	H04N-001/32	
Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC NL PT RO SE SI					
JP 10234012	A		21	H04N-007/08	
US 6104826	A			G06K-009/00	
EP 860984	B1	E		H04N-001/32	
Designated States (Regional): DE FR GB					
DE 69727206	E			H04N-001/32	Based on patent EP 860984
JP 3686741	B2		23	H04N-001/387	Previous Publ. patent JP 10234012

Abstract (Basic): EP 860984 A

The method of watermark-embedding identification information into original **picture** data consisting of pixel values which are arranged in a matrix, the identification information consisting of numerical signals not more than the pixel values. The method comprises generating combinations of basis functions orthogonal each other in association with the numerical signals respectively. Weight coefficients are calculated so that each coefficient corresponds to each of the combinations of the basis functions. For each of the combinations of the basis functions, a sum of products is calculated, for each of the pixels, based on a value of each of the basis functions for a position of the pixel within the original **picture** data and a pixel value of the pixel.

For each of the numerical signals, the method involves referring to a **watermark - embedding function** which is a multi-to-one **function** taking available values of the weight coefficients within a domain and taking available values of the numerical signals within a range, and specifying a input value of the **watermark - embedding function** closest to the weight coefficients calculated for the combinations of the basis functions associated with the numerical signal among several input values of the multi-to-one function outputting a numerical value of the numerical signal. Pixel values in the original **picture data** are **changed** , so that each of the weight coefficients becomes a value equal to the input value which is specified.

USE - E.g. for multi- **media** data to be stored on CDROM or for distribution on network.

ADVANTAGE - Minimises management requirements for identification data. Latter can be extracted without original **image** data.

Dwg.1/11

Title Terms: WATERMARK; EMBED; EXTRACT; IDENTIFY; INFORMATION; **PICTURE** ; DATA; GENERATE; COMBINATION; BASIS; FUNCTION; ORTHOGONAL; NUMERIC; SIGNAL ; COMBINATION; CALCULATE; CORRESPOND; WEIGHT; COEFFICIENT; SUM; PRODUCT; BASIS; FUNCTION; PIXEL; ORIGINAL; **PICTURE**

Derwent Class: T01; W02; W04

International Patent Class (Main): G06K-009/00; H04N-001/32; H04N-001/387; H04N-007/08

International Patent Class (Additional): G06T-001/00; H03M-007/30; H04N-007/081

File Segment: EPI

23/5/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010551541 **Image available**
WPI Acc No: 1996-048494/199605
XRPX Acc No: N96-040696

Digital data processing system for evaluating performance of computer program - has analyser module for analysing binary image **of program and making** modifications **necessary to measure performance and kernel for measuring and storing run time performance information**

Patent Assignee: INTEGRITY SYSTEMS INC (INTE-N)
Inventor: ADAMS S E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5465258	A	19951107	US 89435615	A	19891113	199605	B
			US 9329366	A	19930309		

Priority Applications (No Type Date): US 89435615 A 19891113; US 9329366 A 19930309
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5465258	A		13	G06F-011/34	Cont of application US 89435615

Abstract (Basic): US 5465258 A

The system includes a first computer contg a device for selecting an architecture description file having definitions of boundaries. A device for identifying boundaries performs its operation according to the definitions in the architecture description file in a binary **image** of the computer program.

The system also incorporates a device for **inserting** at the identified boundaries tracking **code** that includes instructions leading to **routines** in a kernel **program** . The routines are adapted for collection of run time performance information, so that a modified binary **image** is created. A second computer includes a device for running the kernel program contg device for running the modified binary **image** .

USE/ADVANTAGE - For evaluating run time performance of computer program. Does not require access source code of program which is analysing.

Dwg.1/15

Title Terms: DIGITAL; DATA; PROCESS; SYSTEM; EVALUATE; PERFORMANCE; COMPUTER; PROGRAM; ANALYSE; MODULE; ANALYSE; BINARY; **IMAGE** ; PROGRAM; MODIFIED; NECESSARY; MEASURE; PERFORMANCE; KERNEL; MEASURE; STORAGE; RUN; TIME; PERFORMANCE; INFORMATION
Derwent Class: T01
International Patent Class (Main): G06F-011/34
File Segment: EPI

23/5/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

008159297 **Image available**
WPI Acc No: 1990-046298/199007
Related WPI Acc No: 1990-139920; 1992-286265
XRPX Acc No: N90-035533

Microcomputer for audio signal processing - is arranged to rewrite contents of filter coefficients RAM without halting multiplication-addition processing using limited capacity RAM

Patent Assignee: NEC CORP (NIDE)
Inventor: KIUCHI T; KLUCHI T
Number of Countries: 005 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 354590	A	19900214	EP 89115012	A	19890814	199007	B
JP 2050611	A	19900220	JP 88201226	A	19880812	199013	
US 5129094	A	19920707	US 89393347	A	19890814	199230	
EP 354590	A3	19920805	EP 89115012	A	19890814	199336	
EP 354590	B1	19970326	EP 89115012	A	19890814	199717	
DE 68927902	E	19970430	DE 627902	A	19890814	199723	
			EP 89115012	A	19890814		

Priority Applications (No Type Date): JP 88201226 A 19880812
Cited Patents: No-SR.Pub; 1.Jnl.Ref; GB 2033624; GB 2155671
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 354590	A	E	14		
Designated States (Regional): DE FR GB					
US 5129094	A		12	G06F-009/38	
EP 354590	B1	E	14	G06F-009/38	
Designated States (Regional): DE FR GB					
DE 68927902	E			G06F-009/38	Based on patent EP 354590

Abstract (Basic): EP 354590 A

When an instruction, WRQ, for **changing** the **contents** of the r filter coefficients RAM (18) is written to the instruction RAM (10), the Qs complement of a flip-flop (42) goes low. If, simultaneously, an external reset signal (136) is applied from a pulse generator (40), the instructions in RAM (10) are executed sequentially.

A HALT signal decoded for an address number, 141, is masked by the AND gate (46) responsive to the output of the flip-flop. Then instructions at addresses 142 to 175 are executed and the coefficients at the corresponding seventeen words in the coefficients RAM are rewritten. Following decoding of address 176 to WRQ signal resets the flip-flop.

ADVANTAGE - Memory requires only memory capacity for storing required amount of coefficients.

1/6

Title Terms: MICROCOMPUTER; **AUDIO** ; SIGNAL; PROCESS; ARRANGE; REWRITING; CONTENT; FILTER; COEFFICIENT; RAM; HALT; MULTIPLICATION; ADD; PROCESS; LIMIT; CAPACITY; RAM
Derwent Class: T01; W04
International Patent Class (Main): G06F-009/38
International Patent Class (Additional): G06F-015/31; H03H-017/02
File Segment: EPI

12/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017164753
WPI Acc No: 2004-672475/200466
XRPX Acc No: N04-533062
Computer program **editing system enciphers machine language code interposed based on starting and completion position identifier words contained in designation file, to calculate parity or** hash **value that is added to executable file**
Patent Assignee: NEC CORP (NIDE)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2004265037	A	20040924	JP 200353512	A	20030228	200466	B

Priority Applications (No Type Date): JP 200353512 A 20030228
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2004265037	A		19	G06F-001/00	

Abstract (Basic): JP 2004265037 A
NOVELTY - An object file (105) is produced from a source file (101). A linker produces an executable file (111) which interposed the machine language code according to starting and completion position identifier words contained in a designation file (109). The interposed code is enciphered to calculate a parity or **hash** value from the **code** , and to **add** the calculated value to an executable file (113).
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(1) computer **program** editing method;
(2) computer **program** editing **program** ; and
(3) computer readable medium storing computer **program** editing **program** .
USE - For editing computer **program** .
ADVANTAGE - The need for **changing** the source file while producing the executable file, is eliminated.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the computer **program** editing system. (Drawing includes non-English language text).
source file 101
object file 105
designation file 109
executable files 111,113
Dwg.1/16
Title Terms: COMPUTER; **PROGRAM** ; EDIT; SYSTEM; ENCIPHER; MACHINE; LANGUAGE ; CODE; INTERPOSED; BASED; START; COMPLETE; POSITION; IDENTIFY; WORD; CONTAIN; DESIGNATED; FILE; CALCULATE; PARITY; **HASH** ; VALUE; ADD; EXECUTE ; FILE
Derwent Class: T01
International Patent Class (Main): **G06F-001/00**
International Patent Class (Additional): **G06F-009/45**
File Segment: EPI

12/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016596281 **Image available**
WPI Acc No: 2004-755015/200474
System and method for controlling certification/use of application program
Patent Assignee: FASOO.COM CO LTD (FASO-N); INST INFORMATION TECHNOLOGY ASSESSMENT (INFO-N)
Inventor: KIM T H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2004061829	A	20040707	KR 200288129	A	20021231	200474	B

Priority Applications (No Type Date): KR 200288129 A 20021231
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2004061829	A		1	G06F-017/00	

Abstract (Basic): KR 2004061829 A
NOVELTY - A system and a method for controlling the certification/use of an **application program** are provided to easily **change** of an operation limit condition of the **application program** , easily manage a version of the **application program** , and prevent an illegal use by easily discriminating the illegal duplication of a library.
DETAILED DESCRIPTION - A **module** certificate generator(210) generates an encrypted **module certificate** template(214) by generating/ **inserting** a **Hash** value of the **application program** (202) into the **module** certificate template(212) having an item for controlling the certification/use of the **application program** , and encrypting/electronically singing the **module** certificate template. A **module** certificate connector(220) connects the encrypted **module** certificate template to the **program** . A **module** certificate confirmer confirms the certification/use of the **application program** by confirming the encrypted **module** certificate template connected to the **application** .
pp; 1 DwgNo 1/10
Title Terms: SYSTEM; METHOD; CONTROL; CERTIFY; APPLY; **PROGRAM**
Derwent Class: T01
International Patent Class (Main): **G06F-017/00**
File Segment: EPI

12/5/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016071534 **Image available**
WPI Acc No: 2004-229395/200422
XRPX Acc No: N04-181436

Sub-objects verification method for data file header object, involves producing digital signature based on data having specific region and array and adding signature **sub-object having array and digital signature to digital object**

Patent Assignee: MICROSOFT CORP (MICT); ADENT D (ADEN-I); CRITES B D (CRIT-I); DUBLISH P (DUBL-I); STROM C P (STRO-I); WEST C (WEST-I)
Inventor: ADENT D; CRITES B D; DUBLISH P; STROM C P; WEST C
Number of Countries: 039 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1396978	A2	20040310	EP 200320076	A	20030904	200422	B
CA 2441620	A1	20040304	CA 2441620	A	20030903	200422	
US 20040054912	A1	20040318	US 2002235587	A	20020904	200422	
EP 1396978	A8	20040623	EP 200320076	A	20030904	200442	
KR 2004021553	A	20040310	KR 200361377	A	20030903	200444	
CN 1490736	A	20040421	CN 2003159313	A	20030903	200446	
AU 2003244037	A1	20040318	AU 2003244037	A	20030901	200450	
BR 200303460	A	20040908	BR 20033460	A	20030904	200462	
JP 2004265380	A	20040924	JP 2003313204	A	20030904	200463	
MX 2003007945	A1	20041001	MX 20037945	A	20030904	200557	

Priority Applications (No Type Date): US 2002235587 A 20020904
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1396978	A2	E	15	H04L-029/06	
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
CA 2441620	A1	E		H04L-012/56	
US 20040054912	A1			H04L-009/00	
EP 1396978	A8	E		H04L-029/06	
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR					
KR 2004021553	A			H04N-007/16	
CN 1490736	A			G06F-015/16	
AU 2003244037	A1			H04L-009/00	
BR 200303460	A			G06F-017/30	
JP 2004265380	A		46	G06F-012/14	
MX 2003007945	A1			G06F-001/00	

Abstract (Basic): EP 1396978 A2

NOVELTY - The method involves creating an array comprising of a region specifier identifying a specific region within a sub-object. A digital signature is produced based on data comprising each specific region and the array. A signature sub-object comprising the array and the digital **signature** is **added** to a digital object. The region specifier comprises a **checksum** calculated based on a **checksum** algorithm.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) a system for use in combination with a digital object

(b) a computer-readable medium for use in combination with a digital object

(c) a memory for storing data for access by an **application program** comprising data structure adapted for storing verification information for an object.

USE - Used for verification of a sub-objects in a header object for a data file in distributed computing environment and general or special

purpose computing system environment e.g. personal computer, server computer, hand-held or laptop device, multiprocessor system, microprocessor based system, set top box, programmable consumer electronics, network PC, minicomputer and mainframe computer.

ADVANTAGE - The sub-object in the header object allows the **modification** of non-protected regions and reorganization of sub-objects in a header without invalidating verification information. The method enables more than one digital signature sub-object to be included in an object, thereby allowing the flexibility in having different areas of sub-objects verified together, and having different entities verify sub-objects.

DESCRIPTION OF DRAWING(S) - The drawing shows a digital signature sub object.

pp; 15 DwgNo 5/5

Title Terms: SUB; OBJECT; VERIFICATION; METHOD; DATA; FILE; HEADER; OBJECT; PRODUCE; DIGITAL; SIGNATURE; BASED; DATA; SPECIFIC; REGION; ARRAY; ADD; SIGNATURE; SUB; OBJECT; ARRAY; DIGITAL; SIGNATURE; DIGITAL; OBJECT

Derwent Class: T01; W01

International Patent Class (Main): **G06F-001/00** ; **G06F-012/14** ; **G06F-015/16** ; **G06F-017/30** ; H04L-009/00; H04L-012/56; H04L-029/06; H04N-007/16

International Patent Class (Additional): **G06F-009/06** ; **G06F-013/00** ; **G06F-017/00** ; G09C-001/00; H04L-009/32; H04L-012/24

File Segment: EPI

12/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015705981 **Image available**
WPI Acc No: 2003-768174/200372
XRPX Acc No: N03-615356

Digital object protecting method, involves creating summary of computed digital signature of digital object by applying cryptographic hash function **or cyclic redundancy check on** signature **and** embedding **summary on object**

Patent Assignee: KONINK PHILIPS ELECTRONICS NV (PHIG); ROBERTS D K (ROBE-I)
Inventor: ROBERTS D K
Number of Countries: 103 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200381896	A1	20031002	WO 2003IB813	A	20030227	200372	B
AU 2003207887	A1	20031008	AU 2003207887	A	20030227	200432	
EP 1491033	A1	20041229	EP 2003704889	A	20030227	200502	
			WO 2003IB813	A	20030227		
KR 2004098025	A	20041118	KR 2004715231	A	20040924	200523	
JP 2005521173	W	20050714	JP 2003579463	A	20030227	200547	
			WO 2003IB813	A	20030227		
US 20050172130	A1	20050804	WO 2003IB813	A	20030227	200552	
			US 2004508564	A	20040922		
CN 1643891	A	20050720	CN 2003807061	A	20030227	200575	

Priority Applications (No Type Date): EP 200276199 A 20020327
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200381896	A1	E	17	H04N-001/32	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
Designated States (Regional): AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT SD SE SI SK SL SZ TR TZ UG ZM ZW

AU 2003207887	A1		H04N-001/32	Based on patent WO 200381896
EP 1491033	A1	E	H04N-001/32	Based on patent WO 200381896

Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR

KR 2004098025	A		H04N-005/913	
JP 2005521173	W	13	G06F-012/14	Based on patent WO 200381896
US 20050172130	A1		H04L-009/00	
CN 1643891	A		H04N-001/32	

Abstract (Basic): WO 200381896 A1

NOVELTY - The method involves computing a digital signature obtained by applying a robust having **function** over contents of a digital object (111). A cryptographic **hash function** or cyclic redundancy check is applied to the computed digital signature to create a summary. The summary is embedded in the object by using a robust watermarking technology.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) a method of verifying the authenticity of a digital watermark
(b) a device for protecting a digital watermark
(c) a device for authenticating digital watermark
(d) a computer **program** product for protecting a digital watermark.

USE - Used for protecting digital objects e.g. images, sound

recordings, audio/video streams.

ADVANTAGE - The cryptographic **hash function** or cyclic redundancy check requires fewer bits to be embedded in the digital object so that small **changes** in the digital object can be identified.

DESCRIPTION OF DRAWING(S) - The drawing shows a schematic diagram of a system for protecting digital objects.

Network (101)

Digital object (111)

Computation **module** (112)

Summarizing **module** (113)

Embedding **module** (114)

pp; 17 DwgNo 1/1

Title Terms: DIGITAL; OBJECT; PROTECT; METHOD; SUMMARY; COMPUTATION; DIGITAL; SIGNATURE; DIGITAL; OBJECT; APPLY; CRYPTOGRAPHIC; **HASH** ; **FUNCTION** ; CYCLIC; REDUNDANT; CHECK; SIGNATURE; EMBED; SUMMARY; OBJECT

Derwent Class: P85; T01; W04

International Patent Class (Main): **G06F-012/14** ; H04L-009/00; H04N-001/32; H04N-005/913

International Patent Class (Additional): G06T-001/00; G09C-001/00; G09C-005/00; H04L-029/06; H04N-001/387; H04N-007/167

File Segment: EPI; EngPI

12/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015374341 **Image available**
WPI Acc No: 2003-435279/200341
XRPX Acc No: N03-347692
Digitized data storing program **for data management system, stores** hash **value of different digitized data to which digital** signature **is** added **to produce digital office data**
Patent Assignee: FUJITSU LTD (FUIT)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2003143139	A	20030516	JP 2001342245	A	20011107	200341	B

Priority Applications (No Type Date): JP 2001342245 A 20011107
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2003143139	A		12	H04L-009/32	

Abstract (Basic): JP 2003143139 A
NOVELTY - A storage unit stores the **hash** value of different digitized data. An assembly unit (13) assembles the stored data. A digital **signature** is **added** to the stored data to produce digital office data. The produced data is written in a storage file using a write-in unit (16).
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for digitized data storage verifying method.
USE - For data management system.
ADVANTAGE - Enables detecting the data **change** , without applying load on system, and guarantees continuity of data.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the digitized data storing **program** . (Drawing includes non-English language text).
assembly unit (13)
write- in unit (16)
pp; 12 DwgNo 1/7
Title Terms: DIGITAL; DATA; STORAGE; **PROGRAM** ; DATA; MANAGEMENT; SYSTEM; STORAGE; **HASH** ; VALUE; DIGITAL; DATA; DIGITAL; SIGNATURE; ADD; PRODUCE; DIGITAL; OFFICE; DATA
Derwent Class: P85; T01; W01
International Patent Class (Main): H04L-009/32
International Patent Class (Additional): **G06F-012/00** ; **G06F-012/14** ; G09C-001/00
File Segment: EPI; EngPI

12/5/18 (Item 18 from file: 347)
DIALOG(R)File 347:JAPIO

06699195 **Image available**
ELECTRONIC DOCUMENT MANAGEMENT SYSTEM, ITS MANAGING METHOD AND COMPUTER READABLE RECORDING MEDIUM RECORDING **PROGRAM** FOR EXECUTING THE METHOD BY COMPUTER

PUB. NO.: 2000-285026 [JP 2000285026 A]
PUBLISHED: October 13, 2000 (20001013)
INVENTOR(s): KANAI YOICHI
APPLICANT(s): RICOH CO LTD
APPL. NO.: 11-093852 [JP 9993852]
FILED: March 31, 1999 (19990331)
INTL CLASS: **G06F-012/14** ; **G0**6F-012/00 ; G09C-001/00; H04L-009/32; **G06F-017/30**

ABSTRACT

PROBLEM TO BE SOLVED: To provide an electronic(E) document management system capable of quickly outputting access permission to a regal user while efficiently preventing the generation of an unapproved access to an E document and the **alteration** of an E document, an E document managing method and a recording medium.
SOLUTION: In the case of storing an E document, a file storage processing part 121a calculates an entry signature by ciphering the **hash** value of a temporary file consisting of the file name of the E document, a document signature obtained by ciphering the document **hash** value of E document data by a private key and an access limitation list by the private key and stores a file entry to which the entry **signature** is **added** in a document management table 126 stored in a large capacity storage medium 105b.

```
Set     Items   Description
S1    2836055   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
           AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2    1125854   INSTRUCTION? ? OR OPERATION? ? OR CODE OR CODING OR CERTIF-
           ICATE? ? OR SIGNATURE? ? OR WATERMARK? ? OR WATER()MARK? ?
S3      61991   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
            OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
           EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)S2
S4      33651   (ADD OR ADDS OR ADDED OR ADDING)(5N)S2
S5    2013831   MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHAN-
           GE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATIO-
           NS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?
S6      81950   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
            HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
           UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
           OR MESSAGE()AUTHENTICATION()CODE OR PARITY
S7     973127   DATA OR FILE OR FILES OR CONTENT? ?
S8    1137423   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
           OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
           PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
           E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?.
           ? OR IMAGE?
S9          20   ((S3 OR S4) (10N) S1) (30N) S5 (30W) S6
S10         20   IDPAT (sorted in duplicate/non-duplicate order)
S11         20   IDPAT (primary/non-duplicate records only)
S12         84   (S3 OR S4) (30N) S1 (30N) S5 (30W) S6
S13         64   S12 NOT S11
S14         48   S13 AND AY=1978:2000
S15         48   IDPAT (sorted in duplicate/non-duplicate order)
S16         47   IDPAT (primary/non-duplicate records only)
S17         22   S12 (30N) S8
S18         16   S17 NOT S11
S19         10   S18 AND AY=1978:2000
S20         10   IDPAT (sorted in duplicate/non-duplicate order)
S21         10   IDPAT (primary/non-duplicate records only)
S22         53   (S3 OR S4) (30N) S1 (30N) (S5 (10N) S6)
S23         33   S22 NOT (S11 OR S21)
S24         24   S23 AND AY=1978:2000
S25         24   IDPAT (sorted in duplicate/non-duplicate order)
S26         24   IDPAT (primary/non-duplicate records only)
S27     194680   S5 (5N)(S7 OR S8)
S28         24   (S3 OR S4) (30N) S1 (30N) S27 (30W) S6
S29          7   S28 NOT (S11 OR S21 OR S26)
S30          7   IDPAT (sorted in duplicate/non-duplicate order)
S31          7   IDPAT (primary/non-duplicate records only)
File 348:EUROPEAN PATENTS 1978-2006/ 200613
         (c) 2006 European Patent Office
File 349:PCT FULLTEXT 1979-2006/UB=20060330,UT=20060323
         (c) 2006 WIPO/Univentio
```

11/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01958897
System, method and program product for checking disclosure of information on network
System, Methode und Programmprodukt fur Prufungsoffenlegung der Informationen uber ein Netzwerk
Systeme, methode et programme pour la verification de revelation d'information sur le reseau
PATENT ASSIGNEE:
Hitachi, Ltd., (5000540), 6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-8280, (JP), (Applicant designated States: all)
INVENTOR:
Moritsu, Toshiyuki Hitachi, Ltd., IP Group New Marunouchi Bldg. 6-1,Marunouchi, 1-chome Chiyoda-ku Tokyo 100-8220, (JP)
Shimamura, Atsushi Hitachi, Ltd., IP Group New Marunouchi Bldg. 6-1,Marunouchi, 1-chome Chiyoda-ku Tokyo 100-8220, (JP)
Takeuchi, Kunihito Hitachi, Ltd., IP Group New Marunouchi Bldg. 6-1,Marunouchi, 1-chome Chiyoda-ku Tokyo 100-8220, (JP)
LEGAL REPRESENTATIVE:
Strehl Schubel-Hopf & Partner (100941), Maximilianstrasse 54, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1580955 A2 050928 (Basic)
APPLICATION (CC, No, Date): EP 2004030736 041223;
PRIORITY (CC, No, Date): JP 200487528 040324
DESIGNATED STATES: AT; BE; BG; CH; CY; CZ; DE; DK; EE; ES; FI; FR; GB; GR; HU; IE; IS; IT; LI; LT; LU; MC; NL; PL; PT; RO; SE; SI; SK; TR
EXTENDED DESIGNATED STATES: AL; BA; HR; LV; MK; YU
INTERNATIONAL PATENT CLASS (V7): H04L-029/06

ABSTRACT EP 1580955 A2
A system for checking disclosure of information on a network, the system includes: a storage device which stores a record including a public location of the information on the network, disclosure start time and disclosure termination time of the information on the network, and disclosed contents of the information on the network; a communication control unit connected to the network, which receives a message including the public location of the pertinent information from the network when the information has been altered; and a processing device which makes access to the public location of the information on the network based on the public location included in the message when the communication control unit has received the message. The communication control unit receives disclosed contents of the pertinent information from the network after altered in accordance with the access by the processing device. And the processing device stores altered time of the pertinent information in a record for the pertinent information before altered in the storage device as disclosure termination time of the pertinent information before altered, and stores altered time of the pertinent information in a record for the information after altered in the storage device as disclosure start time of the pertinent information after altered along with disclosed contents of the information after altered.
ABSTRACT WORD COUNT: 215
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 050928 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200539	2410
SPEC A	(English)	200539	7658

Total word count - document A 10068
Total word count - document B 0
Total word count - documents A + B 10068

...SPECIFICATION a private key 164 which is used for creating a digital signature added to data (**altered** part specification data and **checksums**) to be sent to the certification authority system 120, and a certification authority public key 172A which is used for decoding the digital **signature** **added** to the received content-certification information.

With the **software** and data, and the hardware configuration described above, the information sending system 110 implements functional... alteration inspection program 161 calculates the total value (checksum) of the byte rows of the **alteration** inspection program 161 on the memory 210 as certification data showing its validity, encodes this **checksum** (or the **hash** value of the **checksum**) with the private key 164, and thus creates a digital signature as certification data showing the validity of a sender (S613). Moreover, the **alteration** inspection **program** 161 sends the **checksum** **added** with the digital **signature** to the certification authority system 120 (S614). Here, a digital signature for the **checksum** is created. When one-time challenging data (a random number) is sent from the certification...

...to the certification authority system 120. Thus, spoofing that uses the data sent by the **alteration** inspection program 161 in the past can be prevented.

After that, on the certification authority system 120, when the archiving **program** 181 in the wait state for receiving the **checksum** **added** with the digital **signature** receives message data (S652), it executes a falsification check of the alteration inspection program 161 ...

...altered, the URL of 'file1', 'http://www.hhhh.com/directoryA/file1' is created as the **altered** part specification data 163.

Subsequently, the **alteration** inspection program 161 creates a digital signature for the **altered** part specification data 163 by the same process as that for the digital signature for the **checksum** (S617). Furthermore, the alteration inspection **program** 161 sends the altered part specification data 163 **added** with this digital **signature** to the certification authority system 120 (S618), and returns to the inspection state for the...

11/5,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01452264
A technique for license management and online software license enforcement
Ein Verfahren fur Lizenzverwaltung und online Software-Lizenzerzwingung
Une technique pour la gestion de licences d'utilisation et pour l'application de licences d'utilisation des logiciels en temps reel
PATENT ASSIGNEE:
Fully Licensed GmbH, (4021020), Rudower Chaussee 29, 12489 Berlin, (DE), (Applicant designated States: all)
INVENTOR:
Lopatic, Thomas, Orionstr. 2, 85716 Unterschleissheim, (DE)
LEGAL REPRESENTATIVE:
Korber, Martin, Dipl.-Phys. (88321), Mitscherlich & Partner Patentanwalte Sonnenstrasse 33, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1243998 A1 020925 (Basic)
APPLICATION (CC, No, Date): EP 2001107039 010321;
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): G06F-001/00

ABSTRACT EP 1243998 A1
A software protection is presented comprising software license management and online software license enforcement, wherein individual licenses are provided for regulating the use of a software product, and the software product is individualised while being downloaded from a license server, and the execution of each individualised software product is monitored in agreement with the individual license terms corresponding to the individual software download.
ABSTRACT WORD COUNT: 64
NOTE:
Figure number on first page: 1

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	020925 A1	Published application with search report
Examination:	030507 A1	Date of request for examination: 20030303
Examination:	050309 A1	Date of dispatch of the first examination report: 20050125
Assignee:	050706 A1	Transfer of rights to new applicant: Doboy Inc. (4101501) 869 South Knowles Avenue New Richmond, WI 54017 US
Change:	050706 A1	Legal representative(s) changed 20050520
Assignee:	050713 A1	Transfer of rights to new applicant: Actionality, Inc. (5537960) Corporation Trust Center, 1209 Orange Street Wilmington Delaware 19801, county of New Castle US

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200239	2598
SPEC A	(English)	200239	18466
Total word count - document A			21064
Total word count - document B			0
Total word count - documents A + B			21064

...SPECIFICATION public key when receiving the ticket.
To further increase the level of security, meta-verification **code** is **embedded** to the individual download copy of a piece of **software** in the course of fingerprinting. It makes the verification code tamper-proof by verifying the verification code and uncovering any attempts to **modify**

parts of it. The meta-verification code typically includes **checksum** evaluation over selected parts of the code segment, which contains one or more parts of..

11/5,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00550689
Method for processor simulation.
Verfahren zur Prozessorsimulation.
Procede a simulation d'un processeur.
PATENT ASSIGNEE:
ADVANCED COMPUTER RESEARCH INSTITUTE S.A.R.L., (1506790), 2, Place de la Defense - CNIT, F-92053 Paris La Defense, (FR), (applicant designated states: BE;CH;DE;ES;FR;GB;GR;IT;LI)
INVENTOR:
Katevenis, Manolis, P. Box 1385 (CSI, Forth), GR 711/10 Heraklio, Crete, (GR)
LEGAL REPRESENTATIVE:
de Beaumont, Michel (39716), 1bis, rue Champollion, F-38000 Grenoble, (FR)
PATENT (CC, No, Kind, Date): EP 570646 A1 931124 (Basic)
APPLICATION (CC, No, Date): EP 92420162 920518;
PRIORITY (CC, No, Date): EP 92420162 920518
DESIGNATED STATES: BE; CH; DE; ES; FR; GB; GR; IT; LI
INTERNATIONAL PATENT CLASS (V7): G06F-009/44
CITED PATENTS (EP A): EP 217068 A; EP 327198 A
CITED REFERENCES (EP A):
SIGPLAN '87 (PROCEEDINGS OF THE ACM SYMPOSIUM ON INTERPRETERS AND INTERPRETIVE TECHNIQUE) 11 June 1987, pages 1 - 13 C. MAY 'MIMIC: A Fast System/370 Simulator';

ABSTRACT EP 570646 A1
The invention relates to a translation method ("translation-execution") of foreign binary code not adapted to a host computer. The translation-execution consists in alternately running a translator program (112) to translate a foreign code block of the program into a host code block and running (104) the just translated host block thereafter. The translator will always suspend (106) translation upon reaching a computed Control Transfer Instruction (CTI) as, at translation time, the corresponding computed label cannot be known. The newly translated host block is then run, whereby the host code, corresponding to the foreign code that would be up to then executed, is run. The label of the foreign computed CTI is then effectively computed and can be found in memory. The translator can then resume the translation of the foreign code starting from the computed label. (see image in original document)
ABSTRACT WORD COUNT: 143

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	931124	A1	Published application (A1with Search Report ;A2without Search Report)
Change:	940316	A1	Designated Contracting States (change)
Examination:	940720	A1	Date of filing of request for examination: 940503
Withdrawal:	960605	A1	Date on which the European patent application was deemed to be withdrawn: 951201

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1043
SPEC A	(English)	EPABF1	9970
Total word count - document A			11013
Total word count - document B			0
Total word count - documents A + B			11013

...SPECIFICATION own instructions (code is interpreted as data), such as checksums, as a measure against unauthorized **modification** of the programs. Some other programs, such as self decompressing or self

compiling programs, **modify** themselves. In the former case, the translated programs would perform **checksums** on translated instructions which do not correspond to the same data as the original ones. The **checksums** would thus fail in the translated **programs** . In the latter case, self modifying **instructions** **write** data (corresponding to **instructions**) at specific locations in the code space. The translated self modifying instructions would write exactly...

11/5,K/12 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

01080869 **Image available**
COMPUTER PROGRAM PROTECTION
PROTECTION POUR PROGRAMME INFORMATIQUE
Patent Applicant/Assignee:
BITARTS LIMITED, 3rd Floor, 15 Middle Pavement, Nottingham NG1 7DX, GB, GB (Residence), GB (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
SAFA John Aram, 34 Lenton Road, The Park Estate, Nottingham NG7 1DU, GB, GB (Residence), GB (Nationality), (Designated only for: US)
Legal Representative:
SKINNER Michael Paul (agent), Swindell & Pearson, 48 Friar Gate, Derby DE1 1GY, GB,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200403709 A2-A3 20040108 (WO 0403709)
Application: WO 2003GB2574 20030616 (PCT/WO GB03002574)
Priority Application: GB 200214943 20020628
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PG PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW
(EP) AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5675

English Abstract
Executable **software** (30B) is protected by **inserting** an additional block of **code** (50), immediately after the header (30A). The block (50) is executable to analyse all or part of the structure (30) to determine whether or not any **change** has been made to the structure after the creation of the structure. For example, a **CRC** value may be checked. When the software (30B) is to be executed, the security block (50) executes first, to check if any changes have been made, such as by the effect of a virus. If this is detected, a compressed copy (52) is used to replace at least the program region (30B), prior to execution being handed to the block (30B).

French Abstract
Selon l'invention, un logiciel executable (30B) est protege par insertion d'un bloc de code (50) supplementaire immediatement apres l'en-tete (30A). Le bloc (50) peut etre execute pour analyser l'ensemble ou une partie de la structure (30) afin de verifier si la structure a ete modifiee apres sa creation. Par exemple, une valeur CRC peut etre verifiee. Lorsque le logiciel (30B) doit etre execute, le bloc de securite (50) est execute en premier pour verifier s'il y a eu des modifications, a cause d'un virus, par exemple. Si tel est le cas, une copie compressee (52) est utilisee pour remplacer au moins le domaine du programme (30B), avant que l'execution passe au bloc (30B).

Legal Status (Type, Date, Text)

Publication	20040108	A2 Without international search report and to be republished upon receipt of that report.
Search Rpt	20040415	Late publication of international search report
Republication	20040415	A3 With international search report.
Republication	20040415	A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

English Abstract

Executable **software** (30B) is protected by **inserting** an additional block of **code** (50), immediately after the header (30A). The block (50) is executable to analyse all or part of the structure (30) to determine whether or not any **change** has been made to the structure after the creation of the structure. For example, a **CRC** value may be checked. When the software (30B) is to be executed, the security block...

11/5,K/14 (Item 14 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00835732 **Image available**
A TECHNIQUE FOR PRODUCING, THROUGH WATERMARKING, HIGHLY TAMPER-RESISTANT EXECUTABLE CODE AND RESULTING "WATERMARKED" CODE SO FORMED
TECHNIQUE POUR PRODUIRE PAR APPLICATION DE FILIGRANE DU CODE EXECUTABLE A DEGRE D'INVIOLABILITE ELEVE ET CODE "MARQUE EN FILIGRANE" QUI EN RESULTE

Patent Applicant/Assignee:
MICROSOFT CORPORATION, One Microsoft Way, Redmond, WA 98052, US, US (Residence), US (Nationality)
Inventor(s):
VENKATESAN Ramarathnam, 17208 NE 22nd Ct., Redmond, WA 98052, US,
VAZIRANI Vijay, 801 Atlantic Avenue, Georgia Institute of Technology, College of Computing, Atlanta, GA 30332, US,
Legal Representative:
MICHAELSON Peter L (agent), Michaelson & Wallace, Parkway 109 Office Center, 328 Newman Springs Road, Red Bank, NJ 07701, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200169355 A1 20010920 (WO 0169355)
Application: WO 2001US3821 20010207 (PCT/WO US0103821)
Priority Application: US 2000525694 20000314
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): G06F-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12998

English Abstract
Apparatus and an accompanying method, for forming and embedding a highly tamper-resistant cryptographic identifier, i.e., a watermark, within non-marked executable code, e.g., an application program, to generate a "watermarked" version of that code. Specifically, the watermark, containing, e.g., a relatively large number of separate executable routines, is tightly integrated into a flow pattern of non-marked executable code, e.g., an application program, through randomly establishing additional control flows in the executable code and inserting a selected one of the routines along each such flow. Since the flow pattern of the watermark is highly intertwined with the flow pattern of the non-marked code, the watermak is effectively impossible to either remove from the code and/or circumvent. The routines are added in such a manner that the flow pattern of resulting watermarked code is not substantially different from that of the non-marked code, thus frustrating third party detection of the watermark using, e.g., standard flow analysis tools. To enhance tamper-resistance of the watermarked code, each such routine can provide a pre-defined function such that if that routine were to be removed from the marked code by, e.g., a third party adversary, then the marked code will prematurely terminate its execution.

French Abstract
Appareil et procede correspondant pour former et enfouir un identificateur cryptographique a degre d'inviolabilite eleve, a savoir un filigrane, dans du code executable non marque, tel qu'un programme d'application pour generer une version "marquee en filigrane" de ce code. Le filigrane, qui contient notamment une quantite relativement elevee de routines executables separees, est fortement integre dans un motif de flux d'un code executable non marque tel qu'un programme d'application, et ce au moyen de la creation de flux de commande supplementaires dans le code executable et de l'insertion d'une des routines le long de ce flux. Comme le motif d'ecoulement du filigrane est fortement entrelace avec le motif d'ecoulement du code non marque, il est pratiquement impossible d'extraire le filigrane du code ni de le contourner. Les routines sont ajoutees de maniere a ce que le motif d'ecoulement du code a filigrane ainsi obtenu ne soit pas sensiblement different de celui du code non marque, ce qui empeche les tiers de detecter la presence du filigrane au moyen, par exemple, d'outils standard d'analyse de flux. Pour ameliorer le degre d'inviolabilite du code en filigrane, chaque routine peut assurer une fonction predefinie, de maniere a ce que si cette routine venait a etre retiree du code marque, par exemple, par un tiers hostile, l'execution de ce code marque se terminerait avant terme.

Legal Status (Type, Date, Text)
Publication 20010920 A1 With international search report.
Publication 20010920 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20011108 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... is
associated with an edge inserted, as described below, from GI to HI. A variable **altered** in r2 may be subject to a transformation that undoes that **alteration** , but also in an easily inverted but random looking operation. For example, **routine** r3 may compute a **check - sum** of a pre-defined **code** segment and **write** that sum into a variable in another segment where, e.g., routine r5 is inserted..

11/5,K/17 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00421031 **Image available**
AUTHENTICATION OF SIGNALS USING WATERMARKS
AUTHENTIFICATION DE SIGNAUX A L'AIDE DE FILIGRANES
Patent Applicant/Assignee:
PURDUE RESEARCH FOUNDATION,
WOLFGANG Raymond B,
DELP Edward J III,
Inventor(s):
WOLFGANG Raymond B,
DELP Edward J III,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9811492 A1 19980319
Application: WO 97US16237 19970912 (PCT/WO US9716237)
Priority Application: US 9625589 19960913; US 9737182 19970203
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
JP US AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
Main International Patent Class (v7): G06F-017/30
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 12970

English Abstract
A method of determining if at least a portion of a suspect signal (58) is derived from a watermarked original signal (56) includes the steps of providing a watermark (50) and creating the watermarked original signal (56) by incorporating the watermark (50) onto an original signal (52). At least one first watermark indicator is generated (64) based on the watermarked original signal (56) and the watermark (50) and at least one second watermark indicator is generated (62) based on the suspect signal (58) and the watermark (50). A determination is made (66, 68, 70) whether at least a portion of the suspect signal (58) is derived from the watermarked original signal (56) based on the at least one first watermark indicator (64) and the at least one second watermark indicator (62).

French Abstract
L'invention porte sur une technique permettant d'etablir si au moins une partie d'un signal suspect (58) est derivee d'un signal d'origine porteur d'un filigrane (56). Cette technique consiste a constituer un filigrane (50) et a generer le signal d'origine porteur de filigrane (56) en incorporant le filigrane (50) a ce signal d'origine (52). Il est produit, au moins un premier indicateur de filigrane (64) fonde sur le signal d'origine porteur de filigrane (56) ainsi que sur le filigrane (50), et au moins un second indicateur de filigrane (62) fonde sur le signal suspect ainsi que sur le filigrane (50). Une procedure de determination est alors mise en oeuvre (66, 68, 70) afin d'etablir si une partie, au moins, du signal suspect (58) est derivee du signal d'origine porteur de filigrane (56), cette procedure se fondant sur le premier indicateur de filigrane (64), celui-ci a tout le moins, ainsi que sur le second indicateur de filigrane (62), celui-ci a tout le moins.

Fulltext Availability:
Detailed Description

Detailed Description
... The Video Hash Function 88 supports overlapping watermarks, since the marking procedure does not actually **alter** the original video signal.

Localization can also be achieved by using a secondary watermarking technique such as VW2D. Unlike **checksums** , the **hash** result can be made public without weakening the security of the technique so long as the watermark is kept secret. One approach to using the Video Hash **Function** 88 is to **embed** **watermark** 50 in an EPROM chip (not shown) that is inserted into a video playback device...

11/5,K/18 (Item 18 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00408493 **Image available**
CONDITIONAL ACCESS SYSTEM FOR LOCAL STORAGE DEVICE
SYSTEME D'ACCES CONDITIONNEL POUR UN DISPOSITIF DE MEMORISATION LOCAL
Patent Applicant/Assignee:
SONY ELECTRONICS INC,
LEE Chuen-Chien,
INOUE Hajime,
GOTO Koichi,
Inventor(s):
LEE Chuen-Chien,
INOUE Hajime,
GOTO Koichi,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9749238 A1 19971224
Application: WO 97US7981 19970513 (PCT/WO US9707981)
Priority Application: US 96665893 19960619
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AM AU BA BB BG BR CA CN CU CZ EE GE GH HU IL IS JP KG KP KR LK LR LT LU LV MD MG MK MN MX NO NZ PL RO SG SI SK TR TT UA US UZ VN YU GH KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class (v7): H04N-005/91
International Patent Class (v7): G11B-05:86
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 11375

English Abstract
A technique for selectively inhibiting a video recorder (7) from recording and/or reproducing those television programs, which are not authorized for viewing on the viewing device (8). Authorization data associated with respective television programs that are receivable by the recorder (7) and indication whether that program is authorized for recording and/or reproduction, is received by the recorder (7) or to (or multiplexed with) the television program and is stored thereat. When the television program is received at the receiver (6) and the recorder (7), the stored authorization data associated with that is read to determine if the received television program is authorized for recording and/or reproduction. If not, the recorder (7) is inhibited from recording and/or reproducing that unauthorized television program.

French Abstract
L'invention concerne une technique pour bloquer de maniere selective un magnetoscope (7) et l'empecher d'enregistrer et/ou de reproduire les programmes de television dont la visualisation n'est pas autorisee sur le dispositif de visualisation (8). Des donnees d'autorisation associees aux programmes de television correspondants et pouvant etre recues par l'enregistreur (7) ainsi que des indications precisant si l'enregistrement et/ou la reproduction de ce programme sont autorisees, sont recues par l'enregistreur (7). Elles peuvent egalement etre multiplexees avec le programme ou encore envoyees a ce dernier, puis memorisees. Lorsque le programme de television est recu au niveau du recepteur (6) et de l'enregistreur (7), les donnees d'autorisation memorisees associees sont lues pour determiner si l'enregistrement et/ou la reproduction du programme de television recu sont autorises. Si tel n'est pas le cas, l'enregistreur (7) est bloque et ne peut pas enregistrer et/ou reproduire ce programme de television non autorise.

Fulltext Availability:
  Detailed Description
Detailed Description
... in the storage device where the corresponding program is recorded. Prior to recording the received **modification** keys in the authorization information area, the television receiving apparatus performs error correction **code** encoding, such as **adding** **parity** data.

When a **program** is selected from a local store 45, e,g,, a video tape in the digital...

11/5,K/19 (Item 19 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00385990
METHOD FOR AN ENCRYPTED DIGITAL WATERMARK
PROCEDE RELATIF A UN FILIGRANE NUMERIQUE CODE
Patent Applicant/Assignee:
THE DICE COMPANY,
Inventor(s):
COOPERMAN Marc,
MOSKOWITZ Scott A,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9726733 A1 19970724
Application: WO 97US652 19970117 (PCT/WO US9700652)
Priority Application: US 96587944 19960117
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AL AU BA BB BG BR CA CN CU CZ EE GE HU IL IS JP KP KR LC LK LR LT LV MG MK MN MX NO NZ PL RO SG SI SK TR TT UA UZ VN KE LS MW SD SZ UG AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class (v7): H04L-009/00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 6499

English Abstract
A method for the human-assisted generation and application of pseudo-random keys for the purpose of encoding and decoding digital watermarks to and from a digitized data stream. A pseudo-random key and key application "envelope" are generated and stored using guideline parameters input by a human engineer interacting with a graphical representation of the digitized data stream. Key "envelope" information is permanently associated with the pseudo-random binary string comprising the key. Key and "envelope" information are then applied in a digital watermark system to the encoding and decoding of digital watermarks.

French Abstract
Cette invention concerne un procede de generation et d'application assistees par une personne de cles pseudo-aleatoires, lequel procede permet de coder et de decoder des filigranes numeriques depuis ou vers un flux de donnees numerisees. Une cle pseudo-aleatoire et une "enveloppe" d'application de cle sont generees puis stockees a l'aide de parametres de guidage qui sont entres par un ingenieur se servant de la representation graphique du flux de donnees numerisees. Les informations d'"enveloppe" de cle sont associees en permanence a la chaine binaire pseudo-aleatoire comprenant la cle. On procede ensuite a l'application de la cle et des informations d'"enveloppe" dans un systeme de filigranes numeriques afin de coder et de decoder ces derniers.

Fulltext Availability:
Detailed Description

Detailed Description
... complete watermark certificate, which now contains the checksum, is signed and/or encrypted, which prevents **modification** of any portion of the certificate, including the **checksum** , and finally encoded into the stream. Thus, if it is somehow moved at a later time, that fact can be detected by decoders. once the decoder

functions are separate from the encoder, **watermark** decoding functionality could be **embedded** in several types of **software** including search **agents** , viruses, and automated archive scanners. Such software could then be used to screen files or...

21/5,K/3 (Item 3 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01056405
Electronic watermarking method, electronic information distribution system, image filling apparatus and storage medium therefor
Elektronisches Wasserzeichenverfahren, elektronisches Informationsverteilungssystem, Bildspeicherungsgerat und Speichermedium dafur
Procede de generation de filigrane electronique, systeme de distribution d'information electronique, dispositif d'enregistrement d'image et support d'enregistrement pour ceci

PATENT ASSIGNEE:
CANON KABUSHIKI KAISHA, (542361), 30-2, 3-chome, Shimomaruko, Ohta-ku, Tokyo, (JP), (Applicant designated States: all)
INVENTOR:
Iwamura, Keiichi, Canon Kabushiki Kaisha, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, (JP)
LEGAL REPRESENTATIVE:
Beresford, Keith Denis Lewis et al (28273), BERESFORD & Co. High Holborn 2-5 Warwick Court, London WC1R 5DJ, (GB)
PATENT (CC, No, Kind, Date): EP 932298 A2 990728 (Basic)
EP 932298 A3 000802
APPLICATION (CC, No, Date): EP 99300538 990126;
PRIORITY (CC, No, Date): JP 9813935 980127; JP 9813954 980127; JP 9813955 980127
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04N-001/32; H04L-009/32

ABSTRACT EP 932298 A2
An electronic information distribution system that exchanges data across a network at the least comprises a first entity, including first encryption means, for performing a first encryption process for the original data, a second entity, including management distribution means for, at the least, either managing or distributing the data that are provided by the first encryption process, and including electronic watermark embedding means for embedding an electronic watermark in the data, and a third entity, including second encryption means for performing a second encryption of the data in which an electronic watermark is embedded.
ABSTRACT WORD COUNT: 95
NOTE:
Figure number on first page: 4

LEGAL STATUS (Type, Pub Date, Kind, Text):

Search Report:	000802	A3	Separate publication of the search report
Application:	990728	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	030917	A2	Date of dispatch of the first examination report: 20030806
Examination:	010214	A2	Date of request for examination: 20001218

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9930	3735
SPEC A	(English)	9930	30230
Total word count - document A			33965
Total word count - document B			0
Total word count - documents A + B			33965

...SPECIFICATION which the user must retain, and the second encryption key can be stored in the **image** header portion, while **image** data having an electronic watermark can be stored in the **image** data portion.

In the fourth to the eighth embodiments, electronic **watermark** information can be **embedded** using various methods.

Further, the first encryption and the second encryption can also be implemented by employing various methods, such as an encryption system for **altering** the bit arrangement in consonance with an encryption key. In addition, a **hash** value and its signature can be provided for all data that are to be transmitted. In these embodiments, the first encryption and the second encryption are performed during the electronic **watermark** information **embedding** process in order to prevent the server, the user and the agency from acquiring each other the information stored thereat. However, DES (Data Encryption Standard) cryptography or a hash **function** may be employed to prevent wiretapping and the alteration of data across a communication path...

21/5,K/7 (Item 7 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00903233 **Image available**
METHOD FOR EMBEDDING AND EXTRACTING TEXT INTO/FROM ELECTRONIC DOCUMENTS
PROCEDE PERMETTANT D'INCORPORER DU TEXTE DANS DES DOCUMENTS ELECTRONIQUES ET D'EXTRAIRE DU TEXTE DE CES DERNIERS

Patent Applicant/Assignee:
MARKANY INC, Ssanglim Bldg. 10Fl., 151-11, Ssanglim-Dong, Chung-gu, Seoul 100-400, KR, KR (Residence), KR (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
CHOI Jong Uk, Seong-Won Apt. 2-Dong #1301, Uoo-eui-Dong 1, Dobong-gu, Seoul 142-090, KR, KR (Residence), KR (Nationality), (Designated only for: US)
CHOI Gi Chul, 94-53, Hong-ji-dong, Chongno-gu, Seoul 110-020, KR, KR (Residence), CN (Nationality), (Designated only for: US)
Legal Representative:
KOREANA PATENT FIRM (agent), Dong-Kyong Bldg. 824-19, Yoksam-Dong, Kangnam-gu, Seoul 135-080, KR,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200237309 A1 20020510 (WO 0237309)
Application: WO 2001KR1862 20011102 (PCT/WO KR0101862)
Priority Application: KR 200065038 20001102
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): G06F-017/00
Publication Language: English
Filing Language: Korean
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 8656

English Abstract
The present invention relates to a method and apparatus for authenticating various types of digital certificates by using a text embedding method. The execution of the present invention is divided into two cases, one case including images in the certificate and another case not including the images in the certificate, according to the characteristic of the certificate. In the former case, a text embedding method is applied to images included in the certificate to embed a series of information text (a specific number of the certificate, and issuing organization, name of a person in charge, etc.) designated by a person who issues the certificate into the images. In the latter case, there is generated an image imperceptible to the human eye but having the same color as the ground color of certificate.

French Abstract
L'invention concerne un procede et un dispositif permettant d'authentifier divers types de certificats numeriques au moyen d'un procede d'incorporation de texte. La mise en oeuvre de ce procede comporte deux cas qui dependent du type de certificat: un premier cas comprenant l'inclusion d'images dans le certificat et un second cas ne comprenant pas d'inclusion d'images dans le certificat. Dans le premier

cas, on applique un procede d'incorporation de texte aux images figurant sur le certificat de maniere a incorporer dans les images une serie de textes d'information (un numero specifique de certificat, un organisme d'emission, le nom d'un responsable etc.) specifies par la personne qui delivre le certificat. Dans le second cas, on genere une image imperceptible a l'oeil humain, dont la couleur est identique a la couleur de fond du certificat.

Legal Status (Type, Date, Text)
Publication 20020510 A1 With international search report.

Fulltext Availability:
Detailed Description

Detailed Description
... hash value by the session key S that the person already knows and the hash **function** .

The above hash value is compared with the hash value which -is sent from the...

...its authentication is confirmed and if not, the certificate of authentication is regarded as being **altered** .

Comparison of the **hash** value enables to confirm identity (authentication) of the other party of the transaction and detect whether the certificate is forged or altered. Such authentication using the . authentication **function** has the following drawbacks.

First, authentication is based on a text document. If a document of different forinaf such as an **image** or voice mark is **embedded** into the **certificate** , it should be separately authenticated or its authentication is impossible.

Second, it can accurately determine...

21/5,K/8 (Item 8 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00884006 **Image available**
WATERMARKING RECURSIVE HASHES INTO FREQUENCY DOMAIN REGIONS AND WAVELET BASED FEATURE MODULATION WATERMARKS
INCORPORATION DE FILIGRANES SOUS LA FORME DE HACHAGES RECURSIFS DANS DES REGIONS DU DOMAINE FREQUENTIEL ET FILIGRANES DE MODULATION DE TRAITS A BASE D'ONDELETTES

Patent Applicant/Assignee:
DIGIMARC CORPORATION, Suite 100, 19801 S.W. 72nd Avenue, Tualatin, OR 97062, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
TIAN Jun, Apt. B208, 6455 SW Nyberg Lane, Tualatin, OR 97062, US, US (Residence), CN (Nationality), (Designated only for: US)
DECKER Stephen K, 2530 Orchard Hill Place, Lake Oswego, OR 97035, US, US (Residence), US (Nationality), (Designated only for: US)
BRUNK Hugh L, 2871 SE Kelly St., Portland, OR 97202, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
MEYER Joel R (agent), Digimarc Corporation, Suite 100, 19801 SW 72nd Avenue, Tualatin, OR 97062, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200217214 A2-A3 20020228 (WO 0217214)
Application: WO 2001US26617 20010823 (PCT/WO US0126617)
Priority Application: US 2000645779 20000824; US 2000689293 20001011
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): G06K-009/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 9188
English Abstract
A watermark embedder decomposes a media signal from its perceptual domain to subbands (fig. 2) and embeds a message signal in the edge information of neighboring coefficients of those subbands (fig. 1). A compatible watermark decoder decomposes the watermarked signal into subbands and demodulates the message signal from the edge information of neighboring coefficients.

French Abstract
Dans cette invention, un incorporateur de filigranes decompose en sous-bandes un signal multimedia provenant de son domaine perceptuel et incorpore un signal de message dans les informations marginales des coefficients voisins de ces sous-bandes. Un decodeur de filigranes compatible decompose le signal filigrane en sous-bandes et demodule le signal de message a partir des informations marginales des coefficients voisins. Outre le signal de message, l'incorporateur peut egalement coder un signal d'orientation, afin de synchroniser les decodeurs avec le signal incorpore dans une version distordue du signal filigrane. Ce

systeme de filigranes peut etre utilise dans une grande variete d'applications, telles que le transport robuste de metadonnees ou de liaisons vers des metadonnees et la detection des alterations du signal filigrane, par exemple les alterations dues notamment a l'impression, a la numerisation ou a la compression. Un incorporateur de filigranes transforme en regions du domaine frequentiel un signal multimedia provenant de son domaine perceptuel et incorpore un hachage de donnees a partir d'une region du domaine frequentiel dans un filigrane d'une autre region du domaine frequentiel. Dans une variante, cet incorporateur code des instances du meme message dans ces regions du domaine frequentiel. Pour detecter une alteration du signal multimedia, un decodeur de filigranes transforme un signal suspect en regions du domaine frequentiel, extrait le message de filigranes a partir d'une premiere region du domaine frequentiel et le compare a une reference derivee d'une autre region du domaine frequentiel. Le signal de reference est constitue soit par un hachage calcule a partir de l'autre region du domaine frequentiel du signal filigrane soit par une autre instance du meme message incorpore dans l'autre region du domaine frequentiel. Ce decodeur peut servir a detecter une alteration du signal, telle qu'une alteration se produisant avec des operations de reproduction (impression, numerisation, copiage, conversion N/A-A/N, etc.), de compression, de recadrage ou de permutation d'un contenu de signal multimedia, notamment.

Legal Status (Type, Date, Text)
Publication 20020228 A2 Without international search report and to be republished upon receipt of that report.
Search Rpt 20020530 Late publication of international search report
Republication 20020530 A3 With international search report.
Examination 20021017 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description
... system, such as programmed computer or special purpose forensic analysis tool. For example, a watermarked **image** can be displayed with altered regions in different colors. The extent of the alteration can be color coded so that more severe alterations are distinguishable from less severe ones.

The **watermark** **embedding** fimction described above counters certain types of 1 5 attacks because it is dependent on the host **media** signal. In particular, the embedding **function** modulates edge feature information represented in the relative values of selected groups of neighboring wavelet coefficients. Since these edge features **vary** from one signal to another, it is difficult to copy the watermark from one host signal to another.
More on Using **Watermarks** and **Embedded** **Hashes** to Detect Signal Alteration
Fig. 4 is a flow diagram illustrating a method of **embedding** an authentication **watermark** into frequency domain regions of a **media** signal. The method starts with a **media** object (250) such as an **image** , **video** or **audio** signal, and transforms it into frequency domain regions (252). To illustrate the process, we use...

26/5,K/4 (Item 4 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00981653
Trunking ethernet-compatible networks
Verbindung von Ethernetkompatiblen Netzwerken
Jonction de reseaux compatibles Ethernet
PATENT ASSIGNEE:
Sun Microsystems, Inc., (1392738), 901 San Antonio Road, Palo Alto, California 94303-4900, (US), (Proprietor designated states: all)
INVENTOR:
Hendel, Ariel, 7537 Newcastle Drive, Cupertino, California 95014, (US)
Hejza, Leo A., 1146 Quince Avenue, Sunnyvale, California 94087, (US)
Kumar, Sampath H.K., 491 Galen Drive, San Jose, California 95123, (US)
LEGAL REPRESENTATIVE:
Harris, Ian Richard et al (72231), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)
PATENT (CC, No, Kind, Date): EP 889624 A1 990107 (Basic)
EP 889624 B1 030402
APPLICATION (CC, No, Date): EP 98305137 980629;
PRIORITY (CC, No, Date): US 885072 970630
DESIGNATED STATES: DE; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS (V7): H04L-029/06; H04L-012/56
CITED PATENTS (EP B): EP 863646 A; US 5517488 A; US 5608733 A; US 5633810 A
CITED REFERENCES (EP B):
"LOAD BALANCING FOR MULTIPLE INTERFACES FOR TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL FOR VM/MVS" IBM TECHNICAL DISCLOSURE BULLETIN, vol. 38, no. 9, 1 September 1995, pages 7-9, XP000540166
NISHIZONO T; YOSHIDA Y: "ANALYSIS ON A MULTILINK PACKET TRANSMISSION SYSTEM" ELECTRON. COMMUN. JPN. 1, COMMUN. (USA), vol. 68, no. 9, September 1985, pages 98-104, XP002081618 NEW YORK (US);

ABSTRACT EP 889624 A1
A network system dynamically controls data flow between physical links by logically combining multiple physical links into a single logical channel trunk, preferably to balance data flow carried by each link. Each link in the trunk has identical physical layer and identical media access control layer characteristics. A system server assigns a single media access control layer address to the single trunked logical channel, preferably randomly by hashing destination media access control layer addresses for the links. The system server includes, in addition to a physical layer and a network layer, a pseudo-driver software layer disposed therebetween, which pseudo-driver software layer functions as a multiplexer in a receive path and functions as a de-multiplexer in a transmit path. The resultant preferably Ethernet-compatible network system operates in full-duplex mode and distributes packets from the server to the links to preserve temporal order of data flow.
ABSTRACT WORD COUNT: 145
NOTE:
Figure number on first page: 4A

LEGAL STATUS (Type, Pub Date, Kind, Text):
Examination: 020130 A1 Date of dispatch of the first examination report: 20011213
Application: 990107 A1 Published application (A1with Search Report ;A2without Search Report)
Oppn None: 040324 B1 No opposition filed: 20040105
Grant: 030402 B1 Granted patent
Assignee: 030423 B1 Transfer of rights to new proprietor: Sun Microsystems, Inc. (2616592) 4150 Network Circle Santa Clara, California 95054 US
Examination: 990728 A1 Date of filing of request for examination: 990527
LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199901	594
CLAIMS B	(English)	200314	597
CLAIMS B	(German)	200314	614
CLAIMS B	(French)	200314	729
SPEC A	(English)	199901	10337
SPEC B	(English)	200314	10405
Total word count - document A			10932
Total word count - document B			12345
Total word count - documents A + B			23277

...SPECIFICATION the parameter.
hmedetach
if trunked, deallocates all dynamic data structures allocated for trunk support;
hmeareq
adds code to return error if the device is configured as a non-trunk-head trunk-member;
hme(underscore)trunk(underscore)init
new **function** : wherever hmeinit()is called to **change MAC** parameters/mode, calls hme(underscore)trunk(underscore)init() so that the MAC address, multicast addresses,

promiscuous-mode etc. are set for all trunk-members;
hme trunk(underscore)start
new **function** : wherever hmestart() is currently called to transmit a packet, calls hme trunk(underscore)start() to...

...SPECIFICATION the parameter.
hmedetach
if trunked, deallocates all dynamic data structures allocated for trunk support;
hmeareq
adds code to return error if the device is configured as a non-trunk-head trunk-member;
hme(underscore)trunk(underscore)init
new **function** : wherever hmeinit()is called to **change MAC** parameters/mode, calls hme(underscore)trunk(underscore)init() so that the MAC address, multicast addresses, promiscuous-mode etc. are set for all trunk-members;
hme trunk(underscore)start
new **function** : wherever hmestart() is currently called to transmit a packet, calls hme trunk(underscore)start() to...

26/5,K/7 (Item 7 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00749007
System and method for secure storage and distribution of data using digital signatures
System und Verfahren zur sicheren Speicherung und Verteilung von Daten unter Verwendung digitaler Unterschriften
Systeme et procede pour le stockage securise et la distribution de donnees utilisant des signatures numeriques
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), New Orchard Road, Armonk, N.Y. 10504, (US), (Proprietor designated states: all)
INVENTOR:
Arnold, Todd Weston, 2008 Bantry Lane, Charlotte, NC 28262, (US)
LEGAL REPRESENTATIVE:
Rach, Werner (76871), IBM Deutschland Informationssysteme GmbH, Patentwesen und Urheberrecht, 70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 706275 A2 960410 (Basic)
EP 706275 A3 990630
EP 706275 B1 060125
APPLICATION (CC, No, Date): EP 95113153 950822;
PRIORITY (CC, No, Date): US 306741 940915
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7): H04L-009/32; H04L-009/30;
INTERNATIONAL CLASSIFICATION (V8 + ATTRIBUTES):
IPC + Level Value Position Status Version Action Source Office:
H04L-0009/32 A I F B 20060101 19960104 H EP
H04L-0009/30 A I L B 20060101 19960104 H EP

ABSTRACT EP 706275 A2
The present invention overcomes the disadvantages and limitations of the related art by providing an apparatus and method for secure distribution of software, software updates, and configuration data. Cryptography is used to protect software or data updates sent to computer products or peripherals using non-secure distribution channels. In the preferred embodiment, the contents of the data cannot be read by anyone who obtains the data, and the data will not be accepted unless it is unmodified and originated with the valid source for such data. (see image in original document)
ABSTRACT WORD COUNT: 107
NOTE:
Figure number on first page: 2

LEGAL STATUS (Type, Pub Date, Kind, Text):
Examination: 020227 A2 Date of dispatch of the first examination report: 20020111
Application: 960410 A2 Published application (A1with Search Report ;A2without Search Report)
Grant: 060125 B1 Granted patent
Examination: 961023 A2 Date of filing of request for examination: 960827
Search Report: 990630 A3 Separate publication of the European or International search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) EPAB96 805
CLAIMS B (English) 200604 275
CLAIMS B (German) 200604 275
CLAIMS B (French) 200604 312
SPEC A (English) EPAB96 4907
SPEC B (English) 200604 4249

Total word count - document A 5713
Total word count - document B 5111
Total word count - documents A + B 10824

...CLAIMS the secured area, as the result of said interaction, said specific features which are the **software** updates; and

changing said basic information stored in the memory of the secured area, which change results as part of the interaction of said **program** with the basic information existing before said interaction.

2. The method of claim 1 including the step of: **adding** a **code** to said encrypted data which is to be transferred for the purpose of providing the...

...2, wherein said code is selected from said group consisting of a digital signature, a **modification** detection code (MDC), and a cyclic redundancy check (**CRC**).

4. The method of claim 2 or 3 further including the steps of:authenticating said...

26/5,K/10 (Item 10 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

00353671
Handling of errors in a storage key.
Fehlerverarbeitung in einem Speicherschlussel.
Traitement d'erreurs dans une clef de memoire.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Christensen, Neal Taylor, 23 Brothers Road, Wappingers Falls, NY 12590, (US)
Comfort, Steven Tyler, 39 Parkwood Boulevard, Poughkeepsie, NY 12603, (US)
Hurban, Robert John, 15 Allison Drive, Old Bethpage, NY 11804, (US)
McGilvray, Bruce Lloyd, McAllister Drive, Pleasant Valley, NY 12569, (US)
Sutton, Arthur James, 14 Whitehill Place, Cold Spring, NY 10516, (US)
Urquhart, James Robert, 32 Village Common, Fishkill, NY 12524, (US)
Willoughby, David Ross, 5 Fox Hill 2D, Poughkeepsie, NY 12603, (US)
LEGAL REPRESENTATIVE:
Jost, Ottokarl, Dipl.-Ing. (6092), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht Pascalstrasse 100, W-7000 Stuttgart 80, (DE)
PATENT (CC, No, Kind, Date): EP 371274 A2 900606 (Basic)
EP 371274 A3 920325
APPLICATION (CC, No, Date): EP 89120345 891103;
PRIORITY (CC, No, Date): US 276736 881128
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS (V7): G06F-011/00;
CITED PATENTS (EP A): US 4514847 A; US 4514847 A; US 4942578 A; US 4942578 A
CITED REFERENCES (EP A):
IBM TECHNICAL DISCLOSURE BULLETIN. vol. 22, no. 5, October 1979, NEW YORK US page 2008; BURCHI ET AL.: 'Replacement of SSK instruction in a paging environment'
PATENT ABSTRACTS OF JAPAN vol. 012, no. 345 (P-759)16 September 1988 & JP-A-63 101 948 (FUJITSU) 6 May 1988;

ABSTRACT EP 371274 A2
A method of handling errors in the C bit of a storage key by modifying the INSERT STORAGE KEY (ISK) and the RESET REFERENCE BIT (RRB) instructions. If an error is found in the C bit during the execution of these instructions, microcode is instructed to refresh the C bit. The C bit is interrogated a second time to determine if the refreshed C bit is still in error. If the refreshed C bit is not in error a second time, then the first error was caused by a soft or transient error, and the instruction is continued. If the refreshed C bit is in error a second time then the first and second errors were caused by a permanent error such as a stuck bit, and a system recovery machine check error is generated. The handling of C bit errors is thus done in a dynamic fashion as the instructions are executed. (see image in original document)
ABSTRACT WORD COUNT: 162

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 900606 A2 Published application (A1with Search Report ;A2without Search Report)
Examination: 901122 A2 Date of filing of request for examination: 900926
Search Report: 920325 A3 Separate publication of the European or International search report
Change: 930512 A2 Representative (change)
Withdrawal: 931208 A2 Date on which the European patent application

was deemed to be withdrawn: 930602
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	363
SPEC A	(English)	EPABF1	1844
Total word count - document A			2207
Total word count - document B			0
Total word count - documents A + B			2207

...CLAIMS said change bit (C) on for indicating a value of one, and providing a correct **parity** bit for the turned on **change** bit (C).

3. The method of claim 1 or 2 further comprising, before the refeshing ...

...44).

4. The method of one of claims 1 to 3 wherein said command under **program** control is an **INSERT** STORAGE KEY (ISK) **instruction** (16).

5. The method of claim 4 wherein said testing said change bit (C) is

31/5,K/5 (Item 5 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00960338
CONTENT IDENTIFIERS TRIGGERING CORRESPONDING RESPONSES
IDENTIFICATEURS DE CONTENU DECLENCHANT DES REPONSES CORRESPONDANTES
Patent Applicant/Assignee:
DIGIMARC CORPORATION, 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062, US, US (Residence), US (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
RHOADS Geoffrey B, 2961 SW Turner Road, West Linn, OR 97068, US, US (Residence), US (Nationality), (Designated only for: US)
LEVY Kenneth L, 110 NE Cedar Street, Stevenson, WA 98648, US, US (Residence), US (Nationality), (Designated only for: US)
Legal Representative:
CONWELL William Y (agent), Digimarc Corporation, 19801 SW 72nd Avenue, Suite 100, Tualatin, OR 97062, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200293823 A1 20021121 (WO 0293823)
Application: WO 2002US15187 20020514 (PCT/WO US0215187)
Priority Application: US 2001858189 20010514
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS
LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ
TM TR TT TZ UA UG US UZ VN YU ZA ZM
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class (v7): H04L-009/00
International Patent Class (v7): H04K-001/00
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 2744

English Abstract
Fingerprint data derived from audio or other content is used as an identifier, to trigger machine responses corresponding to the content. The fingerprint can be derived from the content, and also separately encoded in a file header. Digital watermarks can also be similarly used.

French Abstract
Des donnees concernant une empreinte digitale provenant d'un contenu audio ou autre sont utilisees comme identificateurs pour declencher des reponses machine correspondant au contenu. L'empreinte digitale peut provenir du contenu et etre chiffree separement dans un en-tete de fichier. Des filigranes numeriques peuvent etre utilises de facon similaire.

Legal Status (Type, Date, Text)
Publication 20021121 A1 With international search report.
Examination 20030501 Request for preliminary examination prior to end of 19th month from priority date

Fulltext Availability:
Detailed Description

Detailed Description

... should yield the same fingerprint as the same song sampled at 128K. Likewise, a song **embedded** with stegan'ographic **watermark** data should generally yield the same fingerprint as the same song without **embedded** **watermark** data.

One way to do this is to employ a hash **function** that is insensitive to certain **changes** in the input **data** . Thus, two audio tracks that are acoustically similar will **hash** to the same code, notwithstanding the fact -that individual bits are different. A variety of such **hashing** techniques are known.

Another approach does not rely on "hashing" of the audio data

```
Set     Items   Description
S1   15510779   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
             AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2    3860130   INSTRUCTION? ? OR OPERATION? ? OR CODE OR CODING OR CERTIF-
             ICATE? ? OR SIGNATURE? ? OR WATERMARK? ? OR WATER()MARK? ?
S3      30793   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
              OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
             EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)S2
S4      10037   (ADD OR ADDS OR ADDED OR ADDING)(5N)S2
S5    7740432   MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHAN-
             GE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATIO-
             NS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?
S6      79740   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
              HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
             UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
             OR MESSAGE()AUTHENTICATION()CODE
S7    9276719   DATA OR FILE OR FILES OR CONTENT? ?
S8    8125940   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
             OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
             PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
             E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?
             ? OR IMAGE?
S9       2932   (S3 OR S4) AND S1 AND S5
S10        39   S9 AND S6
S11        21   S10 NOT PY>2000
S12        16   RD  (unique items)
File   8:Ei Compendex(R) 1970-2006/Mar W4
         (c) 2006 Elsevier Eng. Info. Inc.
File  35:Dissertation Abs Online 1861-2006/Mar
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Apr 05
         (c) 2006 BLDSC all rts. reserv.
File   2:INSPEC 1898-2006/Mar W4
         (c) 2006 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2006/Jan W2
         (c)2006 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 28
         (c) 2006 The Gale Group
File   6:NTIS 1964-2006/Mar W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Mar W2
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W4
         (c) 2006 Inst for Sci Info
File  62:SPIN(R) 1975-2006/Mar W1
         (c) 2006 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Mar
         (c) 2006 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2006/Apr W1
         (c) 2006 FIZ TECHNIK
File  56:Computer and Information Systems Abstracts 1966-2006/Mar
         (c) 2006 CSA.
File  57:Electronics & Communications Abstracts 1966-2006/Feb
         (c) 2006 CSA.
```

12/5/1 (Item 1 from file: 35)

01530089 ORDER NO: AAD97-04614
MULTIMEDIA SUPPORT IN A WIRELESS MOBILE LOCAL AREA NETWORK
Author: TSAI, TZU-CHIEH
Degree: PH.D.
Year: 1996
Corporate Source/Institution: UNIVERSITY OF CALIFORNIA, LOS ANGELES (0031)
Chair: MARIO GERLA
Source: VOLUME 57/09-B OF DISSERTATION ABSTRACTS INTERNATIONAL. PAGE 5759. 125 PAGES
Descriptors: COMPUTER SCIENCE ; ENGINEERING, ELECTRONICS AND ELECTRICAL
Descriptor Codes: 0984; 0544

The recent common model for wireless, mobile PCS networks is the cellular model: namely, user communicates via radio with base stations which are interconnected via a wired backbone. There is, however, a growing area of mobile, wireless **applications** which will depart from the cellular model, and will require peer to peer communications possibly with multihopping over several mobile stations. Typical **applications** correspond to the situation where a wired infrastructure is not available or is not costeffective to use. Examples include, battlefield, search and rescue, disaster (fire, flood, earthquake) recovery, ad hoc collaborative computing networks, and ad hoc multimedia communications among members of a moving team. In general, the main motivation for wireless multihopping is rapid deployment without need of any existing infrastructure. The multihop networks can be standalone, or can be connected to a wired network.

Basic wireless, mobile, multihop capabilities were demonstrated in the ARPA Packet Radio experiments of the mid 70's. However, those experiments involved only datagram traffic. The protocols did not provide efficient support of real time traffic (voice, video). In this dissertation, we advance the state of the art, in the sense that we address both mobility management and multimedia support in multihopped, wireless networks.

To achieve these goals, we develop the following techniques: (1) Clustering: A distributed, dynamically reconfigurable clustering algorithm partitions the multihop network into clusters so that controlled, accountable bandwidth sharing can be accomplished in each cluster. More specifically, within a cluster, we can easily enforce time-division scheduling. Across clusters, we can facilitate spatial reuse of time slots and codes. (2) TDMA+PRMA channel access scheme: In view of the real time traffic component which requires dedicated bandwidth, VC (Virtual Circuit) connection must guarantee bandwidth and QoS (Quality of Service). Bandwidth guarantee is performed by reserving the time slot(s) in the TDMA frame to each VC. In a highly mobile environment, the conventional VC setup scheme is not suitable because of frequent breakage of the connection. The time required to set up a new VC is comparable to the interval between path **changes** . In order to catch up with station movements, we propose a "soft state", i.e. fast set-up and dynamic rerouting, VC scheme. The first packet in the VC stream follows PRMA (Packet Reservation Multiple Access) scheme to capture and to reserve a slot in the TDMA frame. When the path fails, the PRMA protocol allows the VC stream to dynamically select a new path to destination. (3) QoS routing: To keep track of bandwidth available to each destination is useful to call acceptance control. (4) **Embedded** voice/video **coding** : Low priority substreams are dropped when bandwidth is scarce.

The above techniques span several subnet layers, namely: network layer, topology/connectivity management, **MAC** layer, and physical layer. In order to evaluate the proposed strategy, the entire protocol stack has been implemented in the Maisie simulator. A subset of the protocols was implemented on laptop PCs and tested in a four node testbed.

12/5/7 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

05075312
Title: File Protector (anti-virus program **review)**
Author(s): Jackson, K.
Journal: Virus Bulletin p.25-7
Publication Date: Dec. 1991 Country of Publication: UK
CODEN: VBULE3 ISSN: 0956-9979
U.S. Copyright Clearance Center Code: 0956-9979/91/$0.00+2.50
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Product Review (R)
Abstract: File Protector is an anti-virus **program** which is quite different from competing **software** packages; it works by **adding** a small amount of **code** to each executable file. This code checks that the file has not been **altered** before execution is allowed to proceed. File Protector is an MS-DOS **program** which claims to protect executable files against viruses, or for that matter anything else that attempts to **change** an executable file. In its simplest form, File Protector ensures that the file size, date and time have not been **altered** from when File Protector **code** was first **added** to the executable file. Optionally a **checksum** facility can conduct a thorough byte-by-byte examination of the file. (0 Refs)
Subfile: D
Descriptors: computer viruses; **software** packages
Identifiers: File Protector; anti-virus **program**
Class Codes: D1060 (Security)

12/5/9 (Item 8 from file: 2)
DIALOG(R)File 2:INSPEC

02815821 INSPEC Abstract Number: C82012173
Title: Add **self monitoring to real-time** code
Author(s): O'Flaherty, J.J.
Author Affiliation: Radio Telefis Eireann, Dublin, Ireland
Journal: EDN vol.26, no.20 p.385
Publication Date: 14 Oct. 1981 Country of Publication: USA
CODEN: EDNSBH ISSN: 0012-7515
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: In real-time monitoring and control **applications** , the integrity of **program** code is vital. Marginal EPROMs that partially erase, perhaps due to radiation or delayed print-through of previous code, provide only one example of conditions that can violate this integrity. If the **altered** areas contain rarely entered code, such as alarm **routines** , no problems arise until these **routines** are needed. Such dangerous situations can be avoided by having a **program** monitor its own code. The author describes how to perform this self check with minimal speed or storage penalties, by generating a **checksum** in the **program** 's main loop. (0 Refs)
Subfile: C
Descriptors: **program** testing
Identifiers: self monitoring; real-time code; self check; **checksum**
Class Codes: C6150G (Diagnostic, testing, debugging and evaluating systems)

12/5/11 (Item 1 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04605319 JICST ACCESSION NUMBER: 00A0195356 FILE SEGMENT: JICST-E
A Non-Modal Type of Shift-JIS Text Compression by Using A Dictionary Array.
ITO MASARU (1); SATO TAIJI (2)
(1) Aichi Inst. of Technol.; (2) Yamaguchi Univ.
Denki Gakkai Ronbunshi. C(Transactions of the Institute of Electrical Engineers of Japan. C), 2000, VOL.120-C,NO.1, PAGE.14-19, FIG.1, TBL.10, REF.9
JOURNAL NUMBER: S0810AAN ISSN NO: 0385-4221
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.06
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: This paper proposes a new data compression method for a Japanese-text file, where the text is written in shift-JIS (JIS X 0208) codes. In the first pass, a dictionary array is built up by the higher frequency of both single and double byte characters. In the second pass, all the registered characters are replaced with the dictionary items: the **code** 0xFF is **put into** a compressed file in front of non-registered ASCII character so as to distinguish non-registered characters from registered ones. It takes O(1) time on a **hashing** basis to confirm whether each input character belongs to the dictionary, and to transfer its code to a dictionary item. Furthermore, the run-length encoding is applied to a sequence of consecutive identical characters for the purpose of accomplishment of the much higher compression ratio. The code 0xFE is a indicator to start this encoding. A feature of the method is to be a non-modal type of compression. (author abst.)
DESCRIPTORS: data compression; word processing; document; coding(signal); Japanese
BROADER DESCRIPTORS: data processing; information processing; treatment; computer **application** ; utilization; resource(document); **modification** ; signal processing; oriental language; natural language; language
CLASSIFICATION CODE(S): JD03010Y

12/5/12 (Item 2 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04148604 JICST ACCESSION NUMBER: 99A0562480 FILE SEGMENT: JICST-E
A New Copyright Protection Scheme of Image Using ID-based Signature.
KURIBAYASHI MINORU (1); TANAKA HATSUKAZU (2)
(1) Kobe Univ., Grad. Sch.; (2) Kobe Univ., Fac. of Eng.
Denshi Joho Tsushin Gakkai Gijutsu Kenkyu Hokoku(IEIC Technical Report (Institute of Electronics, Information and Communication Enginners), 1999, VOL.99,NO.57(ISEC99 1-10), PAGE.35-40, FIG.7, TBL.1, REF.5
JOURNAL NUMBER: S0532BBG
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759 681.3:621.397.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: A New copyright protection scheme of images has been proposed using ID-based signature. The scheme dose not bury any unrecognizable proper information like digital **watermark** but **adds** a **signature** for the data sampled based on ID-information to the bottom of image. The copyright transfer is possible by **adding** another new **signature** of the copyrightholder. The copyright transfer of the subimage is also possible. The security of the proposed scheme solely depends on that of the applied ID-based signature scheme. (author abst.)
DESCRIPTORS: digital image; digital signature; identification; copyright; legal protection; DCT(transform); image distortion; signal sampling; **hash function** ; computer simulation; safety; IC card
BROADER DESCRIPTORS: image; cryptogram; recognition; intellectual property; right; protection; cosine transformation; mathematical transformation; mapping(mathematics); transformation and conversion; image quality; image characteristic; characteristic; **modification** ; signal processing ; treatment; **function** (mathematics); computer **application** ; utilization; simulation; property; card(sheet
CLASSIFICATION CODE(S): JD01020V; JE04010I

```
Set     Items   Description
S1   15511028   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
             AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2    3860151   INSTRUCTION? ? OR OPERATION? ? OR CODE OR CODING OR CERTIF-
             ICATE? ? OR SIGNATURE? ? OR WATERMARK? ? OR WATER()MARK? ?
S3      30793   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
              OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
             EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)S2
S4      10037   (ADD OR ADDS OR ADDED OR ADDING)(5N)S2
S5    7740494   MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHAN-
             GE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATIO-
             NS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?
S6     172545   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
              HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
             UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
             OR MESSAGE()AUTHENTICATION()CODE OR PARITY
S7    9276805   DATA OR FILE OR FILES OR CONTENT? ?
S8    8126086   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
             OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
             PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
             E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?
             ? OR IMAGE?
S9        201   S3 AND S1 AND S6
S10        93   S9 NOT PY>2000
S11       128   (S3 AND S1) (50W) S6
S12        61   S11 NOT PY>2000
S13        44   RD  (unique items)
S14        20   (S3 (10N) S1) (50W) S6
S15        16   S14 NOT PY>2000
S16        10   RD  (unique items)
S17    180577   S5 (5N) S7
S18    175235   S5 (5N) S8
S19       335   S3 AND S1 AND (S17 OR S18)
S20       237   S19 AND S8
S21       105   S20 NOT PY>2000
S22        90   (S3 (10N)S1) AND (S17 OR S18)
S23        40   S22 NOT PY>2000
S24        24   RD  (unique items)
File   8:Ei Compendex(R) 1970-2006/Mar W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2006/Mar
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Apr 05
         (c) 2006 BLDSC all rts. reserv.
File   2:INSPEC 1898-2006/Mar W4
         (c) 2006 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2006/Jan W2
         (c)2006 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2006/Mar 29
         (c) 2006 The Gale Group
File   6:NTIS 1964-2006/Mar W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2006/Mar W2
         (c) 2006 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W4
         (c) 2006 Inst for Sci Info
File  62:SPIN(R) 1975-2006/Mar W1
         (c) 2006 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Mar
         (c) 2006 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2006/Apr W1
         (c) 2006 FIZ TECHNIK
File  56:Computer and Information Systems Abstracts 1966-2006/Mar
```

File 57:Electronics & Communications Abstracts 1966-2006/Feb

16/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04485317 E.I. No: EIP96083301200
Title: Compiler-assisted generation of error-detecting parallel programs
Author: Roy-Chowdhury, A.; Banerjee, P.
Corporate Source: IBM T. J. Watson Research Cent, Yorktown Heights, NY, USA
Conference Title: Proceedings of the 1996 26th International Symposium on Fault-Tolerant Computing
Conference Location: Sendai, Jpn Conference Date: 19960625-19960627
Sponsor: IEEE
E.I. Conference No.: 45241
Source: Proceedings - Annual International Conference on Fault-Tolerant Computing 1996. IEEE, Los Alamitos, CA, USA,96CB35969. p 360-369
Publication Year: 1996
CODEN: PFTCDY ISSN: 0731-3071
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review); T; (Theoretical); X; (Experimental)
Journal Announcement: 9610W4
Abstract: We have developed an automated, compile time approach to generating error-detecting parallel programs. The compiler is used to identify statements implementing affine transformations within the **program** and automatically **insert code** for computing, manipulating, and comparing **checksums** in order to detect data errors at runtime. Statements which do not implement affine transformations are checked by duplication. **Checksums** are reused from one loop to the next if this is possible, rather than recomputing **checksums** for every statement. A global dataflow analysis is performed in order to determine points at which checksums need to be recomputed. We also use a novel method of specifying the data distributions of the check data using data distribution directives so that the computations on the original data and the corresponding check computations are performed on different processors. Results on the time overhead and error coverage of the error detecting parallel programs over the original programs are presented on an Intel Paragon distributed memory multicomputer. (Author abstract) 20 Refs.
Descriptors: *Parallel processing systems; Error detection; Program compilers; Parallel algorithms; Fault tolerant computer systems; Encoding (symbols); Data handling; Data reduction; Computational complexity; Time sharing programs
Identifiers: Check sum encoding; Compiler assisted fault tolerance; Error detecting parallel programs
Classification Codes:
722.4 (Digital Computers & Systems); 721.1 (Computer Theory, Includes Formal Logic, Automata Theory, Switching Theory, Programming Theory); 723.1 (Computer Programming); 723.2 (Data Processing)
722 (Computer Hardware); 721 (Computer Circuits & Logic Elements); 723 (Computer Software); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

16/5/7 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

02928636 INSPEC Abstract Number: C82038464
Title: Self-testing embedded parity trees
Author(s): Khakbaz, J.
Author Affiliation: Dept. of Electrical Engng. & Computer Sci., Stanford Univ., Stanford, CA, USA
Conference Title: FTCS 12th Annual International Symposium on Fault-Tolerant Computing. Digest of Papers p.109-16
Publisher: IEEE, New York, NY, USA
Publication Date: 1982 Country of Publication: USA xv+413 pp.
Conference Sponsor: IEEE
Conference Date: 22-24 June 1982 Conference Location: Santa Monica, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P); Theoretical (T)
Abstract: Presents a procedure for modifying embedded parity trees so that they are tested by the inputs they receive during normal, fault-free, operation of the circuit. This eliminates the need for direct control over the input lines of the parity tree for testing purposes. The faults that are detected are single stuck-faults at the terminal lines of the XOR gates in the tree. **Applications** of this procedure to some other **parity** -related **embedded code** checkers are presented. (8 Refs)
Subfile: C
Descriptors: logic testing
Identifiers: self testing; embedded parity trees; single stuck-faults; XOR gates; embedded code checkers
Class Codes: C5210 (Logic design methods)

16/5/8 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1947348 NTIS Accession Number: AD-A302 812/3
Manual and Compiler Assisted Methods For Generating Fault-Tolerant Parallel Programs
(Technical rept)
Roy-Chowdhury, A.
Illinois Univ. at Urbana-Champaign. Coordinated Science Lab.
Corp. Source Codes: 034597093; 097700
Report No.: UILU-ENG-95-2243; CRHC-95-27
Dec 95 130p
Languages: English Document Type: Thesis
Journal Announcement: GRAI9614

NTIS Prices: PC A08/MF A02
Country of Publication: United States
Contract No.: N00014-90-J-1270
We have developed an automated, compile time approach to generating error-detecting parallel programs. The compiler is used to identify statements implementing affine transformations within the **program** and automatically **insert code** for computing, manipulating, and comparing **checksums** in order to check the correctness of the code implementing affine transformations. Statements which do not implement affine transformations are checked by duplication. **Checksums** are reused from one loop to the next if this is possible, rather than recomputing **checksums** for every statement. A global dataflow analysis is performed in order to determine points at which checksums need to be recomputed. We also use a novel method of specifying the data distributions of the check data using directives provided by the High Performance Fortran (HPF) standard so that the computations on the original data and the corresponding check computations are performed on different processors. Results are presented on an Intel Paragon distributed memory multicomputer.
Descriptors: *Software engineering; *Parallel processing; *Fault tolerant computing; Algorithms; Computations; Computers; Theses; Time; Memory devices; Manual operation; Loops; Compilers
Identifiers: Abft(Algorithm based fault tolerance); NTISDODXA
Section Headings: 62B (Computers, Control, and Information Theory--Computer Software)

24/5/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05000140 E.I. No: EIP98044167028
Title: Films as graphical comments in the source code of programs
Author: Mossenbock, Hanspeter
Corporate Source: Johannes Kepler Univ, Linz, Austria
Conference Title: Proceedings of the 1997 Conference on Technology of Object-Oriented Languages and Systems, TOOLS 23
Conference Location: Santa Barbara, CA, USA Conference Date: 19970728-19970801
Sponsor: IEEE
E.I. Conference No.: 48237
Source: TOOLS 23 Proceedings of the Conference on Technology of Object-Oriented Languages and Systems, TOOLS 1997. IEEE Comp Soc, Los Alamitos, CA, USA. p 89-98
Publication Year: 1997
CODEN: 002837
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review); T; (Theoretical)
Journal Announcement: 9806W3
Abstract: We suggest to use animated pictures (films) as graphical comments in the source code of programs. Such pictures can be played forwards and backwards in steps under the control of the user. They can have multiple branches, which lead to different pictures. Animation effects can be applied to show how a **picture changes** over time. This can be useful for visualizing the dynamic behavior of programs. We show how to extend an object-oriented graphics editor so that it can be used for creating and viewing films. We also explain how such films can be **embedded** into the source **code** of **programs** using a text framework. (Author abstract) 11 Refs.
Descriptors: *Three dimensional computer graphics; Codes (symbols); Animation; Object oriented programming; File editors
Identifiers: Animated pictures; Graphical comments; Object oriented graphics editor
Classification Codes:
723.5 (Computer Applications); 723.2 (Data Processing); 723.1 (Computer Programming)
723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

24/5/5 (Item 5 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03838523 E.I. No: EIP94041252975
Title: Rewriting executable files to measure program behavior
Author: Larus, James R.; Ball, Thomas
Corporate Source: Univ of Wisconsin-Madison, Madison, WI, USA
Source: Software - Practice and Experience v 24 n 2 Feb 1994. p 197-218
Publication Year: 1994
CODEN: SPEXBL ISSN: 0038-0644
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications); G; (General Review)
Journal Announcement: 9405W4
Abstract: **Inserting** instrumentation **code** in a **program** is an effective technique for detecting, recording, and measuring many aspects of a program's performance. Instrumentation code can be added at any stage of the compilation process by specially-modified system tools such as a compiler or linker or by new tools from a measurement system. For several reasons, adding instrumentation code after the compilation process - by rewriting the executable file - presents fewer complications and leads to more complete measurements. This paper describes the difficulties in adding code to executable files that arose in developing the profiling and tracing tools qp and qpt. The techniques used by these tools to instrument programs on MIPS and SPARC processors are applicable in other instrumentation systems running on many processors and operating systems. In addition, many difficulties could have been avoided with minor **changes** to compilers and executable **file** formats. These **changes** would simplify this approach to measuring program performance and make it more generally useful. (Author abstract) 24 Refs.
Descriptors: *Program processors; Program compilers; **File** editors; Graph theory; **Modification** ; Computer software; Measurements; Performance
Identifiers: Executable files; Control flow graph
Classification Codes:
723.1 (Computer Programming); 921.4 (Combinatorial Mathematics, Includes Graph Theory, Set Theory)
723 (Computer Software); 921 (Applied Mathematics)
72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS)

24/5/6 (Item 6 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03683007 E.I. No: EIP93081047819

Title: Ddbx-LPP: A dynamic software tool for debugging asynchronous distributed algorithms on loosely coupled parallel processors

Author: Fernandez, Mariano G.; Ghosh, Sumit
Corporate Source: Brown Univ, Providence, RI, USA

Source: Journal of Systems and Software v 22 n 1 Jul 1993. p 27-43
Publication Year: 1993
CODEN: JSSODM ISSN: 0164-1212
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications); G; (General Review)
Journal Announcement: 9310W1

Abstract: It is generally accepted in the parallel processing community that powerful yet flexible debuggers are indispensable for the efficient programming of complex distributed synchronous and asynchronous algorithms on loosely coupled parallel processors. Traditional debugging systems, including POKER, permit a user to start, stop, and single-step a parallel program executing on a parallel processor while observing the successive changes of the traced variables and labels. These debuggers are limited in that the user must specify the list of variables and labels to be traced through the declaration section of each routine. As a result, the user may not **alter** the **contents** of this set once program execution has been initiated. More recently, debuggers such as ndb and dbxtool claim dynamic debugging support but are limited by clumsy user interfaces. While ndb works within a single window and requires the user to type commands, dbxtool is a simple collection of uniprocessor debuggers with no explicit coordination. PROVIDE claims to use graphical tools for debugging but is limited to a simplified programming language. Furthermore, both ndb and dbxtool are proprietary; few details, if any, on their software engineering design are available in the literature. This article details the software engineering issues in the design and implementation of an actual distributed dynamic runtime software debugger, Ddbx-LPP, that permits the user to view any global variable, structure, and parameter during program execution at any node of a parallel processor system. The system is exclusively mouse driven for relatively easy debugging. The user may **insert** breakpoints corresponding to any source **code** line, either before initiating execution or when **program** execution is temporarily suspended at a breakpoint. Furthermore, when the program, in the course of execution, experiences a nonrecoverable error, its execution is temporarily suspended and control is transferred to the user in a manner identical to the case of a deliberately inserted breakpoint. Although further execution is prohibited, Ddbx-LPP permits the user to view variables and structures to determine the cause of the error. Ddbx-LPP's unique ability may be credited to its significant analysis of the object code and symbol table, generated as a result of compilation under the ?-g' option, both before and during the actual execution of the program. In contrast to POKER, which requires a sequential programming environment, Ddbx-LPP may function with a user program written in C for any loosely coupled parallel processor. Ddbx-LPP is superior to user-inserted ?printf' statements to print out the values of variables and structures during execution because 1) to print all variables and structures would require an overwhelming number of printf statements, and 2) to insert new printf statements would mean program recompilation. Ddbx-LPP has been implemented on the ARMSTRONG system at Brown University and is equally applicable to any loosely coupled parallel processor system. (Author abstract) 28 Refs.

Descriptors: *Parallel processing systems; Program debugging; Algorithms; Computer aided software engineering; Distributed computer systems; Codes (symbols); Data structures
Identifiers: Asynchronous distributed algorithms; Distributed dynamic runtime software debugger Ddbx-LPP; Brown University

Classification Codes:
722.4 (Digital Computers & Systems); 723.1 (Computer Programming);
723.5 (Computer Applications)
722 (Computer Hardware); 723 (Computer Software)
72 (COMPUTERS & DATA PROCESSING)

24/5/7 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01811599 ORDER NO: AADAA-I3001407
Optimal rate allocation and security schemes for image and video transmission over wireless channels
Author: Song, Jie
Degree: Ph.D.
Year: 2000
Corporate Source/Institution: University of Maryland College Park (0117)
Adviser: K. J. Ray Liu
Source: VOLUME 62/01-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 445. 136 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL
Descriptor Codes: 0544
ISBN: 0-493-10037-7

In this dissertation, we study several issues for image and video coding and transmission over wireless networks which include optimal source and channel rate allocation, error resilient video coding, and key distribution schemes for secure multimedia multicast.

We propose a progressive image transmission scheme in the case of transmission over broadband wireless channels using multiple antennas and orthogonal frequency division multiplexing (OFDM). By employing multiple antennas and OFDM, we transfer the frequency selective, time varying fading channels to parallel Gaussian noisy channels when the number of antennas is large enough, as a result, the forward error control (FEC) coding can be more effective and the source throughput is increased.

We propose an integrated framework of optimal rate allocation for video coding in the case of transmission over wireless channels without feedback channel available. For a fixed channel bit rate and finite number of channel coding rate, the proposed scheme can find out the optimal source and channel coding pair and corresponding robust video coding scheme such that the expected end-to-end distortion of video signals can be minimized. With the assumption that encoder has the stochastic information of the channel model, the proposed scheme takes into account video coding, channel coding and packetization, error concealment techniques altogether.

We also propose a novel data embedding scheme for fractional-pixel based video coding algorithms such as H.263 and **MPEG** -2. By **modifying** the motion estimation procedure at fractional-pel precision, two bits data can be embedded in a motion vector for a Inter-mode coded macroblock. As an **application** example of the proposed data **embedding** scheme, an error-resilient video **coding** scheme is also presented. The proposed scheme has better error recovery performance than previous methods because of this embedded coding scheme.

Another important problem considered in this dissertation is security for multimedia multicast such as video conferencing and pay-per-view. We propose a new key management scheme for the distribution of multicast rekeying message. Furthermore, we present a new key distribution scheme for multimedia multicast by exploiting the characteristics of multimedia signals such that key updating messages can be hidden in the data and used in conjunction with encryption to protect the multimedia data from unauthorized access.

24/5/8 (Item 2 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01745646 ORDER NO: AADAA-I9972109
Methods for improved robustness of image watermarking algorithms
Author: Liang, Te-shen
Degree: Ph.D.
Year: 2000
Corporate Source/Institution: The University of Arizona (0009)
Director: Jeffrey J. Rodriguez
Source: VOLUME 61/05-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 2684. 114 PAGES
Descriptors: ENGINEERING, ELECTRONICS AND ELECTRICAL ; COMPUTER SCIENCE
Descriptor Codes: 0544; 0984
ISBN: 0-599-77385-5

With the advent of multimedia technology and the popularity of Internet communications, there has been great interest in using digital watermarks for the purpose of copy protection and content authentication. Digital watermarking technology allows the content owner to **embed** a secret **signature** , i.e., **watermark** , into the host content for many **applications** . For digital watermarking, the major challenge lies in the confident verification of the embedded watermark, even after the watermarked content undergoes various forms of unintentional or malicious modification. Approaches aiming to guarantee reliable verification of an imperceptible watermark are termed robust watermarking algorithms.

In this dissertation, we study digital image watermarking and provide more robust algorithms toward reliable watermark verification, assuming various types of "content-preserving" image processing. Three new algorithms based on attack analysis, spectrum equalization, and a modified embedding rule are proposed. We discuss and analyze the proposed solutions, and compare them thoroughly against conventional algorithms. Since the watermark robustness is to be tested under various forms of image processing, the watermark encoder can utilize the knowledge of some possible attacks for a more secure embedding. Our first solution toward robust image watermarking is to select the set of best watermarking coefficients through attack analysis using the un-watermarked, original image.

For transform-domain algorithms, the discrete cosine transform (DCT) or discrete wavelet transform (DWT) are normally used for decomposing the host image before embedding the watermark. Due to the low-pass characteristic of most **images** , the DCT/DWT coefficients generally **vary** in amplitude throughout the **image** spectrum. This low-pass nature is an advantage for many transform coders, but it does not facilitate a reliable watermark extraction for many watermarking algorithms. Our second solution for a more robust watermarking is the use of a simple, invertible permutation operator to equalize the transform coefficients before watermarking.

Many transform-domain schemes utilize a directly-proportional rule for embedding the watermark. This approach results in diminishing performance as the watermark capacity increases. Our third solution provides a new embedding scheme that is inversely dependent on the magnitude of the selected transform coefficients. This scheme enhances performance, enabling a large-capacity watermark.

24/5/10 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

07405335 INSPEC Abstract Number: C1999-12-6160-006
Title: Code generation for integrity constraint check in Objectivity/C++
Author(s): In-Tae Kim; Ki-Chang Kim; Sang-Bong U; Sang-Kyun Cha
Journal: Journal of KISS(C) (Computing Practices) vol.5, no.4 p. 416-25
Publisher: Korea Inf. Sci. Soc,
Publication Date: Aug. 1999 Country of Publication: South Korea
CODEN: CKNCFY ISSN: 1226-2293
SICI: 1226-2293(199908)5:4L.416:CGIC;1-U
Material Identity Number: E347-1999-006
Language: Korean Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: To cope with the complexity of handling integrity constraints, numerous researchers have suggested to use a rule-based system, where integrity constraints are expressed as rules and stored in a rule base. A rule manager and an integrity constraint manager cooperate to check the integrity constraints efficiently. In this approach, however, the integrity constraint manager has to monitor the activity of an application program constantly to catch any database operation. For each database operation, it has to check relevant rules with the help of the rule manager, resulting in considerable delays in database access. We propose to insert the constraints checking code in the **application program** directly at compile time. With constraints checking **code inserted** , the **application program** can check integrity constraints by itself without the intervention of the integrity constraint manager. We investigate what kind of statements require the checking of constraints, show how the compiler can detect those statements, and show how constraints checking **code** can be **inserted** into the **program** , by **modifying** the GCC YACC **file** for Objectivity/C/sup ++/, an object-oriented database programming language. (20 Refs)
Subfile: C
Descriptors: C++ language; data integrity; database management systems; knowledge based systems; program compilers
Identifiers: code generation; integrity constraint check; Objectivity/C++ ; rule-based system; rule manager; integrity constraint manager; database operation; database access; constraints checking code; GCC YACC file; object-oriented database programming language
Class Codes: C6160 (Database management systems (DBMS)); C6150C (Compilers, interpreters and other processors); C6140D (High level languages); C6110J (Object-oriented programming); C6170 (Expert systems and other AI software and techniques)

24/5/11 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

07147298 INSPEC Abstract Number: C1999-03-6130S-012
Title: The "ticket" concept for copy control based on embedded signalling
Author(s): Linnartz, J.P.M.G.
Author Affiliation: Philips Res. Lab., Eindhoven, Netherlands
Conference Title: Computer Security - ESORICS 98. 5th European Symposium on Research in Computer Security. Proceedings p.257-74
Editor(s): Quisquater, J.-J.; Deswarte, Y.; Meadows, C.; Gollmann, D.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1998 Country of Publication: Germany x+375 pp.
ISBN: 3 540 65004 0 Material Identity Number: XX-1998-02642
Conference Title: Computer Security - ESORICS 98. 5th European Symposium on Research in Computer Security
Conference Date: 16-18 Sept. 1998 Conference Location: Louvain-la-Neuve, Belgium
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: This **application** -oriented paper discusses the use of electronic **watermarks** (also called **embedded** signaling) for copy control. Playback control and copy-once are described. The ticket concept is presented to provide these functionalities. Although the ticket shows similarities with a digital signature, there are essential differences. For instance, the ticket allows typical **modifications** of the **content** , which are common practice in transmission, storage and presentation of video. The concept is part of a proposal under investigation for standardization of DVD/CPTWG copy control. This paper also compares the ticket concept with other solutions, such as embedding a secondary mark at the recorder and using a signature scheme. (8 Refs)
Subfile: C
Descriptors: copy protection; cryptography; industrial property; multimedia systems; security of data; standardisation; video discs
Identifiers: copy control; embedded signalling; electronic watermarks; playback control; copy-once; ticket concept; digital signature; video transmission; video storage; video presentation; standardization; DVD; CPTWG; signature scheme; multimedia
Class Codes: C6130S (Data security); C0230 (Economic, social and political aspects of computing); C6130M (Multimedia)

```
Set     Items   Description
S1   22469944   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
              AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2     102951   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
               OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
              EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)(INSTRUCTION? ?
               OR OPERATION? ? OR CODE OR CODING OR CERTIFICATE? ? OR SIGNA-
              TURE? ? OR W
S3     164019   (ADD OR ADDS OR ADDED OR ADDING)(5N)(INSTRUCTION? ? OR OPE-
              RATION? ? OR CODE OR CODING OR CERTIFICATE? ? OR SIGNATURE? ?
              OR WATERMARK? ? OR WATER()MARK? ?)
S4     683980   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
               HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
              UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
              OR MESSAGE()AUTHENTICATION()CODE OR PARITY
S5      18705   (MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHA-
              NGE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATI-
              ONS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?)(1-
              0N)S4
S6     222999   (DATA OR FILE OR FILES OR CONTENT? ?)(3N)(MODIFY OR MODIFI-
              ES OR MODIFYING OR MODIFICATION? ? OR CHANGE? ? OR CHANGING OR
               VARY OR VARIES OR VARYING OR VERIFICATIONS? ? OR ALTER? ? OR
              ALTERED OR ALTERING OR ALTERATION? ?)
S7   18157523   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
              OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
              PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
              E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?
              ? OR IMAGE?
S8           1   ((S2 OR S3) (10N) S1) (30N) S6 (30W) S4
S9           3   ((S2 OR S3) (10N) S1) (30N) S5
S10          2   ((S2 OR S3) (30N) S1) (30N) S6 (30W) S4
S11        342   ((S2 OR S3) (10N) S1) (30W) S4
S12         54   S11 (30N) S7
S13         48   S12 NOT PY>2000
S14         30   RD  (unique items)
S15         30   S14 NOT (S8 OR S9 OR S10)
File  88:Gale Group Business A.R.T.S. 1976-2006/Mar 30
         (c) 2006 The Gale Group
File 369:New Scientist 1994-2006/Aug W4
         (c) 2006 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2006/Apr 06
         (c) 2006 ProQuest Info&Learning
File  15:ABI/Inform(R) 1971-2006/Apr 06
         (c) 2006 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2006/Apr 06
         (c) 2006 The Gale Group
File   9:Business & Industry(R) Jul/1994-2006/Apr 05
         (c) 2006  The Gale Group
File  13:BAMP 2006/Mar W4
         (c) 2006  The Gale Group
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2006/Apr 05
         (c) 2006 Business Wire.
File 647:CMP  Computer Fulltext 1988-2006/Apr W4
         (c) 2006 CMP Media, LLC
File  98:General Sci Abs 1984-2004/Dec
         (c) 2005 The HW Wilson Co.
File 148:Gale Group Trade & Industry DB 1976-2006/Apr 06
         (c)2006 The Gale Group
File 634:San Jose Mercury  Jun 1985-2006/Apr 05
         (c) 2006 San Jose Mercury News
File 275:Gale Group Computer DB(TM) 1983-2006/Apr 05
```

(c) 2006 The Gale Group
File 47:Gale Group Magazine DB(TM) 1959-2006/Apr 06
(c) 2006 The Gale group
File 75:TGG Management Contents(R) 86-2006/Mar W4
(c) 2006 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2006/Apr 05
(c) 2006 The Gale Group
File 624:McGraw-Hill Publications 1985-2006/Apr 06
(c) 2006 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2006/Apr W1
(c) 2006 ProQuest
File 613:PR Newswire 1999-2006/Apr 06
(c) 2006 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Dec
(c) 2005 The HW Wilson Co
File 239:Mathsci 1940-2006/May
(c) 2006 American Mathematical Society
File 370:Science 1996-1999/Jul W3
(c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2006/Apr 05
(c) 2006 Dialog
File 553:Wilson Bus. Abs. 1982-2006/Apr
(c) 2006 The HW Wilson Co

15/3,K/22 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

07234410 SUPPLIER NUMBER: 15332218 (USE FORMAT 7 OR 9 FOR FULL TEXT)
VIP-C version 1.0.2. (Mainstay) (Software Review) (one of three evaluations of rapid application development software in 'RAD II') (Evaluation)
DelRossi, Robert A.; Quinn, Stephen R.; Gale, Bob; Spragens, John
InfoWorld, v16, n17, p87(5)
April 25, 1994
DOCUMENT TYPE: Evaluation ISSN: 0199-6649 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1734 LINE COUNT: 00132

...ABSTRACT: with ANSI specifications, and can also interpret user-supplied lines. A library of standard C **functions** is included with VIP-C; this deals mainly with **inserting** **code** templates into a **program** . However, the package also translates over 3,000 low-level **Mac** Toolbox calls into 600 high-level functions grouped into such categories as events, math, **graphics** and strings. VIP-C's main drawback is its lack of database connectivity for any...

15/3,K/26 (Item 8 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

04498697 SUPPLIER NUMBER: 08147096 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Pixar to bring 3-D rendering to the Macintosh. (product announcement)
Bernard, Diane
PC Week, v7, n6, p33(2)
Feb 12, 1990
DOCUMENT TYPE: product announcement ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 376 LINE COUNT: 00031

...ABSTRACT: its Renderman ($995) software in Mar 1990. The company plans to join with third-party **software** developers to showcase upcoming **Mac applications** with **embedded** Renderman **code** at the National Computer **Graphics** Association. These **applications** will allow **Mac** users to add texture and light-source shadings to color and three-dimensional geometric models...

8/3,K/1 (Item 1 from file: 148)

05172026 SUPPLIER NUMBER: 10703482 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Systems librarian and automation review.
Schuyler, Michael
Computers in Libraries, v11, n3, p28(6)
March, 1991
ISSN: 1041-7915 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 5539 LINE COUNT: 00411

... program that keeps track of the size changes, you know something has happened to that **program** .

Another method of attack is for the virus to **write** itself into the existing **code** of a file. The **file** size doesn't **change** at all, but some of the bytes in the file are different.

One way to defend against this type of virus is to include a cyclical redundancy check (**CRC**) on the bytes of the file itself. This means a program will read every byte...

```
Set     Items   Description
S1      28381   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
          AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API
S2       5988   INSTRUCTION? ? OR OPERATION? ? OR CODE OR CODING OR CERTIF-
          ICATE? ? OR SIGNATURE? ? OR WATERMARK? ? OR WATER()MARK? ?
S3        137   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
           OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
          EDDED OR IMBEDDING OR WRITE? ? OR WRITTING)(5N)S2
S4         89   (ADD OR ADDS OR ADDED OR ADDING)(5N)S2
S5       4125   MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHAN-
          GE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATIO-
          NS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ?
S6        482   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
           HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
          UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK? OR MAC
          OR MESSAGE()AUTHENTICATION()CODE OR PARITY
S7      18147   DATA OR FILE OR FILES OR CONTENT? ?
S8      11341   MEDIA OR MULTIMEDIA OR  AUDIO? OR VIDEO? ? OR RECORDING? ?
          OR STREAM? OR MP3 OR MP4 OR WMA OR WINDOWS()MEDIA()AUDIO OR M-
          PEG? ? OR MPG? ? OR JPEG? ? OR JPG? ? OR MOVIE? ? OR MINIMOVI-
          E? ? OR FILM? ? OR PICTURE? ? OR GRAPHIC? ? OR MUSIC OR GAME?
          ? OR IMAGE?
S9          0   (S3 OR S4) AND S1 AND S5 AND S6
S10         2   (S3 OR S4) AND S1 AND S6
S11        39   (S3 OR S4) AND S1 AND S5
S12        39   RD  (unique items)
S13         9   S11 AND S8
S14         0   S12 NOT RD>20000307
S15        51   (S3 OR S4) AND S1 AND S8
S16         2   S15 NOT RD>20000307
File 256:TecInfoSource 82-2006/Apr
         (c) 2006 Info.Sources Inc
```

16/5/1
DIALOG(R)File 256:TecInfoSource

02769266 DOCUMENT TYPE: Company

Actions Semiconductor Co Ltd (769266)
15-1 #1 HIT Rd Tangjia, Zhuhai
Guangdong, CH 519085 China
TELEPHONE: (86) 756-3392353
FAX: (86) 756-3392251
HOMEPAGE: http://www.actions.com.cn
EMAIL: info@actions.com.cn
TICKER: NASDAQ : ACTS

RECORD TYPE: Directory

CONTACT: Sales Department

ORGANIZATION TYPE: Corporation
EQUITY TYPE: Public
STATUS: Active

Actions Semiconductor Company Limited, founded in 2001 and based in Zhuhai, China, is a fabless semiconductor company that is known for its system-on-a-chip (SoC) products. The firm's technology is employed in **MP3** and other personal **media** players. Actions Semiconductor products support the capture, storage, and playback of digital **audio** , **image** , and **video** files. The company's SoC systems work with flash memory and HDD players. The chips provide users with straightforward integration and low power consumption features. Actions Semiconductor technology includes **audio** encoding, digital rights management, USB and Bluetooth connectivity, and **audio** post-processing support features. Controllers support color LCDs. SoCs packages provide original equipment manufacturers (OEMs) with **software** development kits (SDKs). The SDKs include **embedded** firmware **code** , development tools, and documentation. The firm also develops energy metering SoC products. Actions Semiconductor went public in 2005. The firm is listed on NASDAQ under the ACTS symbol. The company employs 260 people, including 130 engineers. It was registered in the Cayman Islands in 2001. In 2003, the China Semiconductor Industry Association (CSIA) identified Actions Semiconductor as having the best growth potential of all circuit design development firm's in China. Actions Semiconductor is expanding its SoC product line and focusing on expanding alliances with **MP3** manufacturers in China. It plans to expand its research and development engineering staff. In 2004, the firm spent $2.4 million on research.

SALES: NA
DATE FOUNDED: 2001

DESCRIPTORS: Consumer Electronics; Embedded Systems; SoC (Systems on Chips)
REVISION DATE: 00000000

```
et     Items   Description
S1       372   AU=(JAKUBOWSKI M? OR JAKUBOWSKI, M?)
S2       780   AU=(VENKATESAN R? OR VENKATESAN, R?)
S3      1135   S1 OR S2
S4  17999186   FUNCTION? ? OR PROGRAM? ? OR SOFTWARE OR APPLICATION? ? OR
             AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API OR INSTRUCTION? ? -
             OR OPERATION? ? OR CODE? ? OR CODING
S5       355   S3 AND S4
S6    157360   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
              OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
             EDDED OR IMBEDDING OR ADD OR ADDS OR ADDED OR ADDING)(5N)S4
S7         1   S5 AND S6
S8    560895   (MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHA-
             NGE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATI-
             ONS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ? )(-
             10N)S4
S9        20   S5 AND S8
S10       19   S9 NOT PY>2000
S11       10   RD  (unique items)
S12      185   S5 NOT PY>2000
S13    45098   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
              HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
             UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK?
S14       30   S5 AND S13
S15       30   S14 NOT (S7 OR S11)
S16       19   S15 NOT PY>2000
S17        9   RD  (unique items)
File   2:INSPEC 1898-2006/Mar W4
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W4
         (c) 2006 Inst for Sci Info
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Mar
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Apr 05
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Jan W2
         (c)2006 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Mar
         (c) 2006 The HW Wilson Co.
File 144:Pascal 1973-2006/Mar W2
         (c) 2006 INIST/CNRS
File 636:Gale Group Newsletter DB(TM) 1987-2006/Apr 04
         (c) 2006 The Gale Group
```

```
et     Items   Description
S1       372   AU=(JAKUBOWSKI M? OR JAKUBOWSKI, M?)
S2       780   AU=(VENKATESAN R? OR VENKATESAN, R?)
S3      1135   S1 OR S2
S4  17999186   FUNCTION? ? OR PROGRAM?. ? OR SOFTWARE OR APPLICATION? ? OR
             AGENT? ? OR ROUTINE? ? OR MODULE? ? OR API OR INSTRUCTION? ? -
             OR OPERATION? ? OR CODE? ? OR CODING
S5       355   S3 AND S4
S6    157360   (INSERT?? OR INSERTING OR EMBED? ? OR EMBEDDED OR EMBEDDING
              OR (PUT OR PUTS OR PUTTING)()(IN OR INTO) OR IMBED? ? OR IMB-
             EDDED OR IMBEDDING OR ADD OR ADDS OR ADDED OR ADDING)(5N)S4
S7         1   S5 AND S6
S8    560895   (MODIFY OR MODIFIES OR MODIFYING OR MODIFICATION? ? OR CHA-
             NGE? ? OR CHANGING OR VARY OR VARIES OR VARYING OR VERIFICATI-
             ONS? ? OR ALTER? ? OR ALTERED OR ALTERING OR ALTERATION? ? )(-
             10N)S4
S9        20   S5 AND S8
S10       19   S9 NOT PY>2000
S11       10   RD  (unique items)
S12      185   S5 NOT PY>2000
S13    45098   CHECKSUM? ? OR CHECK()SUM? ? OR HASH OR HASHES OR HASHED OR
              HASHING OR MD5 OR SHA OR MESSAGE()DIGEST(3W)(5 OR FIVE OR FO-
             UR OR 4) OR MD4 OR CRC OR CYCLICAL()REDUNDANCY()CHECK?
S14       30   S5 AND S13
S15       30   S14 NOT (S7 OR S11)
S16       19   S15 NOT PY>2000
S17        9   RD  (unique items)
File   2:INSPEC 1898-2006/Mar W4
         (c) 2006 Institution of Electrical Engineers
File   6:NTIS 1964-2006/Mar W4
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2006/Mar W4
         (c) 2006 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2006/Mar W4
         (c) 2006 Inst for Sci Info
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2006/Mar
         (c) 2006 ProQuest Info&Learning
File  65:Inside Conferences 1993-2006/Apr 05
         (c) 2006 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2006/Jan W2
         (c)2006 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Mar
         (c) 2006 The HW Wilson Co.
File 144:Pascal 1973-2006/Mar W2
         (c) 2006 INIST/CNRS
File 636:Gale Group Newsletter DB(TM) 1987-2006/Apr 04
         (c) 2006 The Gale Group
```

7/5/1 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

15387820 PASCAL No.: 02-0076385
A graph theoretic approach to software **watermarking**
IH 2001 : information hiding : Pittsburgh PA, 25-27 April 2001
VENKATESAN Ramarathnam ; VAZIRANI Vijay; SINHA Saurabh
MOSKOWITZ Ira S, ed
Microsoft Research, Unknown; Georgia Tech, United States; University of Washington, United States
Information hiding. International workshop, 4 (Pittsburgh PA USA) 2001-04-25
Journal: Lecture notes in computer science, 2001, 2137 157-168
ISBN: 3-540-42733-3 ISSN: 0302-9743 Availability: INIST-16343; 354000097039770120
No. of Refs.: 20 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany
Language: English

We present a graph theoretic approach for watermarking **software** in a robust fashion. While watermarking **software** that are small in size (e.g. a few kilobytes) may be infeasible through this approach, it seems to be a viable scheme for large **applications** . Our approach works with control/data flow graphs and uses abstractions, approximate k-partitions, and a random walk method to embed the watermark, with the goal of minimizing and controlling the additions to be made for embedding, while keeping the estimated effort to undo the watermark (WM) as high as possible. The watermarks are so **embedded** that small changes to the **software** or flow graph are unlikely to disable detection by a probabilistic algorithm that has a secret. This is done by using some relatively robust graph properties and error correcting **codes** . Under some natural assumptions about the **code added** to **embed** the WM, locating the WM by an attacker is related to some graph approximation problems. Since little theoretical foundation exists for hardness of typical instances of graph approximation problems, we present heuristics to generate such hard instances and, in a limited case, present a heuristic analysis of how hard it is to separate the WM in an information theoretic model. We describe some related experimental work. The approach and methods described here also suitable for solving the problem of **software** tamper resistance.

English Descriptors: Problem solving; Heuristic method; Random walk; Partition method; Error correcting **code** ; **Coding** ; Fluence graph; Data flow; Graph theory; Watermarking

French Descriptors: Resolution probleme; Methode heuristique; Marche aleatoire; Methode partition; **Code** correcteur erreur; Codage; Graphe fluence; Flot donnee; Theorie graphe; Filigranage

Classification Codes: 001D04A04E

11/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

06757148 INSPEC Abstract Number: A9801-9260-014
Title: Modeling wind field and pollution transport over a complex terrain using an emergency dose information code **SPEEDI**
Author(s): **Venkatesan, R.** ; Mollmann-Coers, M.; Natarajan, A.
Author Affiliation: Safety Res. & Health Phys. Group, Indira Gandhi Centre for Atomic Res., Kalpakkam, India
Journal: Journal of Applied Meteorology vol.36, no.9 p.1138-59
Publisher: American Meteorol. Soc,
Publication Date: Sept. 1997 Country of Publication: USA
CODEN: JAMOAX ISSN: 0894-8763
SICI: 0894-8763(199709)36:9L.1138:MWFP;1-I
Material Identity Number: J201-97010
U.S. Copyright Clearance Center Code: 0894-8763/97/$4.25+0.25
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: Atmospheric dispersion **code** system SPEEDI (System for prediction of environmental emergency dose information) has been applied to simulate the field experiments conducted over a complex terrain, a diagnostic mass-consistent wind field model of the **code** system simulates the flow over an isolated hill using the routinely measured data from sodars and a meteorological tower. An objective basis for the adjustment of the horizontal and vertical wind components has been incorporated in the model, and the results show a great improvement in modeling the flow past the hill. Calculated profiles of the vertical velocity component around the hill have been compared with those observed by the sodars. The model streamlines show close agreement with the tetroon trajectory and the ground-level concentration patterns. Dispersion calculations are carried out using a Lagrangian particle random walk model. The dispersion algorithm is modified in order to utilize the observed turbulence data instead of the conventional Pasquill-Gifford method, and the former scheme performs better in simulating the concentration distribution. Results suggest that the accuracy of the **code** system improves significantly when all these **changes** are introduced. (14 Refs)
Subfile: A
Descriptors: air pollution; atmospheric boundary layer; atmospheric movements; atmospheric radioactivity; radioactive pollution; wind
Identifiers: atmosphere; boundary layer; air pollution; radioactivity; radioactive pollution; accident; accidental release; wind field; pollution transport; complex terrain; emergency dose information **code** ; SPEEDI; land surface topography; System for prediction of environmental emergency dose information; hill; ground-level concentration pattern; dispersion; Lagrangian particle random walk model
Class Codes: A9260T (Air quality and air pollution); A8670G (Atmosphere (environmental science)); A9260F (Atmospheric boundary layer structure and processes); A9260E (Convection, turbulence, and diffusion in the lower atmosphere); A9260G (Winds and their effects in the lower atmosphere)

11/5/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

06671912 INSPEC Abstract Number: C9710-6130S-005
Title: Threat-adaptive security policy
Author(s): **Venkatesan, R.M.** ; Bhattacharya, S.
Author Affiliation: Dept. of Electr. & Comput. Eng., Arizona State Univ., Tempe, AZ, USA
Conference Title: 1997 IEEE International Performance, Computing and Communications Conference (Cat. No.97CH36051) p.525-31
Publisher: IEEE, New York, NY, USA
Publication Date: 1997 Country of Publication: USA 578 pp.
ISBN: 0 7803 3873 1 Material Identity Number: XX97-00827
U.S. Copyright Clearance Center Code: 0 7803 3873 1/97/$10.00
Conference Title: 1997 IEEE International Performance, Computing and Communications Conference
Conference Sponsor: IEEE; IEEE Commun. Soc
Conference Date: 5-7 Feb. 1997 Conference Location: Phoenix, Tempe, AZ, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Secure systems have traditionally paid little attention to performance. This is because current secure systems apply a uniform and statically decided upon security policy to each user and do not associate an individualized level of trust with each user at run-time. This paper describes a new framework of threat and performance driven security. A threat-adaptive model which enforces a dynamic and individualized security policy mechanism, with a trust state machine capturing the different security levels is proposed. This paper discusses a threat-adaptive firewall designed for an EC **application** , which adaptively **varies** the security constraints for each user, thereby improving the system performance. (7 Refs)
Subfile: C
Descriptors: authorisation; finite state machines; security of data; **software** performance evaluation
Identifiers: threat-adaptive security policy; performance; run-time; trust state machine; threat-adaptive firewall; EC **appl**ication ; intrusion detection
Class Codes: C6130S (Data security); C4220 (Automata theory)

11/5/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

06239828 INSPEC Abstract Number: A9610-8670G-007
Title: Application **of a refined emergency** code **system SPEEDI to atmospheric field experiments conducted over a complex terrain**
Author(s): **Venkatesan, R.** ; Mollmann-Coers, M.
Author Affiliation: Safety Res. & Health Phys. Group, Indira Gandhi Centre for Atomic Res., Kalpakkam, India
Journal: Journal of Nuclear Science and Technology vol.33, no.2 p. 157-65
Publisher: Atomic Energy Soc. Japan,
Publication Date: Feb. 1996 Country of Publication: Japan
CODEN: JNSTAX ISSN: 0022-3131
SICI: 0022-3131(199602)33:2L.157:AREC;1-5
Material Identity Number: J006-96004
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: An environmental emergency **code** system SPEEDI consisting of a mass consistent wind field model and a lagrangian particle dispersion model is taken up for validation study using the benchmark data obtained from a series of field experiments conducted over a complex terrain. During the experiments extensive data on meteorological parameters were collected and in addition SF/sub 6/ tracer gas was released and sampled by thickly distributed samplers. An isolated hill placed on an otherwise flat terrain provides a special geometrical situation so that the data can be used for testing the model simulation of stream line deflections past an obstacle. An objective basis for relating the ratio of Gauss precision moduli which controls the horizontal to vertical adjustment of the wind components has been introduced in the wind field model and the results show great improvement particularly when the parameter is allowed to vary with height. Results of the tracer release experiments confirm the improvements. The modified wind field model is then coupled with the lagrangian particle dispersion model. Diffusion calculations are carried out using locally obtained empirical diffusion parameters similar to the traditional Pasquill-Gifford parameters and as well as the observed turbulence information. Better accuracy is seen in the calculation of tracer concentration distribution in the latter case. While the **code** retains the merit of quick and effective use of **routine** measurements, the general performance is expected to improve when these **changes** are incorporated in it. (12 Refs)
Subfile: A
Descriptors: air pollution; environmental science computing; fission reactor accidents; radioactive pollution; wind
Identifiers: SPEEDI; atmospheric field experiments; complex terrain; environmental emergency **code** system; lagrangian particle dispersion model ; SF/sub 6/ tracer gas; hill; Gauss precision moduli; wind; wind field model; Pasquill-Gifford parameters; turbulence; nuclear accident; SF/sub 6
Class Codes: A8670G (Atmosphere (environmental science)); A9260G (Winds and their effects in the lower atmosphere)
Chemical Indexing:
SF6 bin - F6 bin - F bin - S bin (Elements - 2)

11/5/5 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1939343 NTIS Accession Number: TIB/B96-00477
Simulation of the wind field and pollution transport over a complex terrain using an emergency dose information code **SPEEDI**
Venkatesan, R. ; Moellmann-Coers, M.
Forschungszentrum Juelich G.m.b.H. (Germany, F.R.). Abt. Sicherheit und Strahlenschutz.
Corp. Source Codes: 096982009; 9203981
Report No.: JUEL--3095
Jul 95 55p
Languages: English
Journal Announcement: GRAI9609
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC E09
Country of Publication: Germany, Federal Republic of
Atmospheric dispersion **code** system SPEEDI (System for Prediction of Environmental Emergency Dose Information) has been applied to simulate the field experiments conducted over a complex terrain. Two series of tracer release expperiments conducted during stable atmospheric cnditions have been considered for the present study. A diagnostic mass consistent wind field model of the **code** system simulates the flow over an isolated hill using the routinely measured data from SODARs and meteorological tower. An objective basis for the adjustment of the horizontal and vertical wind components has been incorporated in the model and the results show a great improvement in modelling the flow past the hill. Calculated profiles of the vertical velocity component around the hill have been compared with those observed by the SODARs. The model stream lines show closer agreement with the tetroon trajectory and the ground level concentration patterns. Dispersion calculations are carried out using a Lagrangian particle random walk model and the dispersion parameters obtained from the earlier local field experiment are used in the model. The **code** is modified in order to utilise the observed turbulence data and the later scheme performs better in simulating high values of the concentrations observed near the source. Summary of the results of all the cases suggests that the accuracy of the **code** system improves significantly when all these **changes** are introduced. Problems yet to be resolved characteristics of this terrain are also discussed in this report. (orig.). (Copyright (c) 1996 by FIZ. Citation no. 96:000477.)
Descriptors: *Meteorology; *Computerized simulation; *Pollution transport ; *Wind (meteorology); *Terrain; *Superpressure balloons; Dispersions; Diffusion; Complex terrain; Wind; Radioactivity transport; Air pollution; Flow distribution
Identifiers: *Foreign technology; NTISTFFIZ
Section Headings: 55B (Atmospheric Sciences--Dynamic Meteorology); 68A (Environmental Pollution and Control--Air Pollution and Control); 68F (Environmental Pollution and Control--Radiation Pollution and Control); 57V (Medicine and Biology--Radiobiology)

17/5/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

08011473 INSPEC Abstract Number: B2001-09-6135C-346, C2001-09-6160S-108
Title: Robust image hashing
Author(s): **Venkatesan, R.** ; Koon, S.-M.; **Jakubowski, M.H.** ; Moulin, P.
Author Affiliation: Cryptography Group, Microsoft Corp., Redmond, WA, USA
Conference Title: Proceedings 2000 International Conference on Image Processing (Cat. No.00CH37101) Part vol.3 p.664-6 vol.3
Publisher: IEEE, Piscataway, NJ, USA
Publication Date: 2000 Country of Publication: USA 3 vol.(lxviii+1027+957+1000) pp.
ISBN: 0 7803 6297 7 Material Identity Number: XX-2001-00128
U.S. Copyright Clearance Center Code: 0 7803 6297 7/2000/$10.00
Conference Title: Proceedings of 7th IEEE International Conference on Image Processing
Conference Sponsor: IEEE Signal Process. Soc
Conference Date: 10-13 Sept. 2000 Conference Location: Vancouver, BC, Canada
Medium: Also available on CD-ROM in PDF formt
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T); Experimental (X)
Abstract: The proliferation of digital images creates problems for managing large image databases, indexing individual images, and protecting intellectual property. This paper introduces a novel image indexing technique that may be called an image **hash function** . The algorithm uses randomized signal processing strategies for a non-reversible compression of images into random binary strings, and is shown to be robust against image changes due to compression, geometric distortions, and other attacks. This algorithm brings to images a direct analog of message authentication **codes** (MACs) from cryptography, in which a main goal is to make **hash** values on a set of distinct inputs pairwise independent. This minimizes the probability that two **hash** values collide, even, when inputs are generated by an adversary. (10 Refs)
Subfile: B C
Descriptors: cryptography; database indexing; error correction **codes** ; image **coding** ; image representation; industrial property; transform **coding** ; visual databases; wavelet transforms
Identifiers: robust image **hashing** ; digital images; large image database management; image indexing; intellectual property protection; image **hash function** ; randomized signal processing; nonreversible image compression; random binary strings; geometric distortions; image changes; image attacks; message authentication **codes** ; cryptography; **hash** values collision probability; wavelet representation; error correcting **codes** ; statistical properties

Class Codes: B6135C (Image and video coding); B0290X (Integral transforms in numerical analysis); B6120D (Cryptography); C6160S (Spatial and pictorial databases); C6130S (Data security); C5260B (Computer vision and image processing techniques); C4188 (Integral transforms in numerical analysis); C1260C (Cryptography theory)

17/5/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

07489860 INSPEC Abstract Number: B2000-03-6120D-048, C2000-03-1260C-034
Title: High-speed pseudorandom number generation with small memory
Author(s): Aiello, W.; Rajagopalan, S.; **Venkatesan, R.**
Author Affiliation: Res., ATT Labs., Florham Park, NJ, USA
Conference Title: Fast Software Encryption. 6th International Workshop, FSE'99. Proceedings p.290-304
Editor(s): Knudsen, L.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1999 Country of Publication: Germany viii+316 pp.
ISBN: 3 540 66226 X Material Identity Number: XX-1999-02370
Conference Title: Fast Software Encryption. 6th International Workshop, FSE'99
Conference Date: 24-26 March 1999 Conference Location: Rome, Italy
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We present constructions for a family of pseudorandom generators that are very fast in practice, yet possess provable strong cryptographic and statistical unpredictability properties. While such constructions were previously known, our constructions here have much smaller memory requirements, e.g., small enough for smart cards, etc. Our memory improvements are achieved by using variants of pseudorandom **functions** . The security requirements of this primitive are a weakening of the security requirements of a pseudorandom **function** . We instantiate this primitive by a keyed secure **hash function** . A sample construction based on DES and **MD5** was found to run at about 20 Mbit/s on a Pentium II. (22 Refs)
Subfile: B C
Descriptors: cryptography; random number generation; smart cards; statistical analysis; storage allocation
Identifiers: high-speed pseudorandom number generation; memory size; cryptographic properties; statistical unpredictability; smart cards; security requirements; keyed secure **hash function** ; DES; **MD5** ; Pentium II
Class Codes: B6120D (Cryptography); B0240Z (Other topics in statistics); C1260C (Cryptography theory); C5230 (Digital arithmetic methods); C6130S (Data security); C1140Z (Other topics in statistics)

17/5/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

06992343 INSPEC Abstract Number: B9809-6120B-104, C9809-6130S-064
Title: The chain and sum primitive and its applications to MACs and stream ciphers
Author(s): **Jakubowski, M.H.** ; **Venkatesan, R.**
Author Affiliation: Princeton Univ., NJ, USA
Conference Title: Advances in Cryptology - EUROCRYPT '98. International Conference on the Theory and Application of Cryptographic Techniques. Proceedings p.281-93
Editor(s): Nyberg, K.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1998 Country of Publication: Germany x+606 pp.
ISBN: 3 540 64518 7 Material Identity Number: XX98-01341
Conference Title: Advances in Cryptology - EUROCRYPT '98 International Conference on the Theory and Applications of Cryptographic Techniques Proceedings
Conference Sponsor: Int. Assoc. Cryptologic Res
Conference Date: 31 May-4 June 1998 Conference Location: Espoo, Finland
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We present a new scheme called universal block chaining with sum (or chain and sum primitive (C and S) for short), and show its **application** to the problem of combined encryption and authentication of data. The primitive is a weak CBC-type encryption along with a summing step, and can be used as a front-end to stream ciphers to encrypt pages or blocks of data (e.g., in an encrypted file system or in a video stream). Under standard assumptions, the resulting encryption scheme provably acts as a random permutation on the blocks, and has message integrity features of standard CBC encryption. The primitive also yields a very fast message authentication **code** (MAC), which is a multivariate polynomial evaluation **hash** . The multivariate feature and the summing aspect are novel parts of the design. Our tests show that the chain and sum primitive adds approximately 20 percent overhead to the fastest stream ciphers. (16 Refs)
Subfile: B C
Descriptors: block **codes** ; combinatorial mathematics; cryptography; data integrity; message authentication; polynomials
Identifiers: chain and sum primitive; stream ciphers; universal block chaining; data authentication; weak CBC-type encryption; random permutation ; provable security; message integrity; message authentication **code** ; multivariate polynomial evaluation **hash**
Class Codes: B6120B (Codes); B0250 (Combinatorial mathematics); C6130S (Data security); C1160 (Combinatorial mathematics)

17/5/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

06959393 INSPEC Abstract Number: B9808-6120B-050, C9808-6130S-045
Title: New constructions for secure hash functions
Author(s): Aiello, W.; Haber, S.; **Venkatesan, R.**
Conference Title: Fast Software Encryption. 5th International Workshop, FSE'98 Proceedings p.150-67
Editor(s): Vaudenay, S.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1998 Country of Publication: Germany viii+296 pp.
ISBN: 3 540 64265 X Material Identity Number: XX98-00615
Conference Title: Fast Software Encryption 5th International Workshop, FSE '98 Proceedings
Conference Date: 23-25 March 1998 Conference Location: Paris, France
Language: English Document Type: Conference Paper (PA)
Treatment: New Developments (N); Theoretical (T)
Abstract: Presents new schemes for the construction of collision-resistant **hash functions** and analyzes some simple methods for combining existing **hash function** designs so as to enhance their security. We first map the input to a slightly longer string using secure stretch **functions** . These are length-increasing, almost-surely injective one-way **functions** that sufficiently randomize their inputs so that it is hard for an adversary to force the outputs to fall into a target set. Then we apply a compression **function** to the output of the stretch **function** . We analyze the security of these constructions under different types of assumptions on both stretch and compression **functions** . These assumptions combine random- **function** models, the intractability of certain "biasing" tasks and the degeneracy structure of compression **functions** . The use of stretching allows reduced requirements on the compression **function** . These constructions allow one to use efficient primitives that may exhibit weaknesses as collision-resistant **functions** , but no attacks are currently known on their one-way and randomizing properties when they are used as stretch **functions** as in our constructions. Our use of stretch **functions** enables us to base our compression **function** on DES so that the resulting **hash function** achieves practical speeds. We also suggest some imperfect random-oracle models, showing how to build better primitives from given imperfect ones. We also analyze how to defend against a collision-finding adversary for a given primitive by building independent primitives. (37 Refs)
Subfile: B C
Descriptors: computability; cryptography; **functions**
Identifiers: secure **hash functions** ; collision-resistant **hash functions** ; secure stretch **functions** ; length-increasing almost-surely injective one-way **functions** ; string length; input randomization; compression **functions** ; random- **function** models; intractability; biasing tasks; degeneracy structure; efficient primitives; cryptoattacks; randomizing properties; DES; Data Encryption Standard; imperfect random-oracle models; collision-finding adversary; independent primitives
Class Codes: B6120B (Codes); C6130S (Data security)

17/5/5 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

06828705 INSPEC Abstract Number: B9803-6120B-111, C9803-6130S-037
Title: Highly parallel cryptographic attacks
Author(s): Peinado, M.; **Venkatesan, R.**
Author Affiliation: Inst. for Algorithms & Sci. Comput., Nat. Res. Center for Inf. Technol., St. Augustin, Germany
Conference Title: Recent Advances in Parallel Virtual Machine and Message Passing Interface. 4th European PVM/MPI Users' Group Meeting. Proceedings p.367-74
Editor(s): Bubak, M.; Dongarra, J.; Wasniewski, J.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1997 Country of Publication: Germany xv+518 pp.
ISBN: 3 540 63697 8 Material Identity Number: XX97-02731
Conference Title: Recent Advances in Parallel Virtual Machine and Message Passing Interface. 4th European PVM/MPI Users Group Meeting. Proceedings
Conference Date: 3-5 Nov. 1997 Conference Location: Cracow, Poland
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We report on a large-scale statistical evaluation of pseudo-random properties of certain cryptographic **functions** such as DES and **MD5** . The evaluation is based on the well-known birthday attack. The attack requires large amounts of memory. We describe a parallel algorithm which can exploit the large amounts of secondary memory (local disks) available on many workstation clusters and parallel machines. The overheads due to communication and disk accesses can be minimized by techniques similar to those used in parallel data bases for parallel external sorting. We have implemented the algorithm using the message passing interface MPI. We display performance measurements on an IBM SP2 which show that the costs for communication and disk accesses are negligible. (18 Refs)
Subfile: B C
Descriptors: cryptography; message passing; parallel algorithms
Identifiers: highly parallel cryptographic attacks; large-scale statistical evaluation; pseudo-random properties; cryptographic **functions** ; DES; **MD5** ; birthday attack; parallel algorithm; secondary memory; local disks; workstation clusters; parallel databases; message passing interface; MPI; IBM SP2
Class Codes: B6120B (Codes); C6130S (Data security); C4240P (Parallel programming and algorithm theory)

17/5/6 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

06329227 INSPEC Abstract Number: B9609-6120B-031, C9609-6130S-022
Title: Foiling birthday attacks in length-doubling transformations
Author(s): Aiello, W.; **Venkatesan, R.**
Author Affiliation: Math. & Cryptography Res. Group, Bell Commun. Res., Morristown, NJ., USA
Conference Title: Advances in Cryptology - EUROCRYPT '96. International Conference on the Theory and Application of Cryptographic Techniques. Proceedings p.307-20
Editor(s): Maurer, U.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1996 Country of Publication: West Germany xii+416 pp.
ISBN: 3 540 61186 X Material Identity Number: XX96-01253
Conference Title: Advances in Cryptology - EUROCRYPT '96
Conference Sponsor: Int. Assoc. Cryptologic Res
Conference Date: 12-16 May 1996 Conference Location: Saragossa, Spain
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: For many cryptographic primitives, e.g., **hashing** and pseudorandom **functions** and generators, doubling the output length is useful even if the doubling transformation is not reversible. For these cases, we present a non-reversible construction based on a Benes network, as an alternative to the traditional Feistel construction (which is the basis of DES). Assuming that a given primitive behaves like an n-bit to n-bit random **function** , we present a length-doubling scheme that yields a 2n-bit to 2n-bit **function** that probably requires Omega (2/sup n/) queries to distinguish with theta (1) probability from a truly random **function** of that length. This is true even if the adversary is of unlimited computing power and is allowed to query the **function** adaptively. Our construction is minimal in the sense that omitting any **operation** makes the resulting network susceptible to birthday attacks using O(2/sup n/2/) queries. Feistel networks also use truly random n-bit **functions** to achieve 2n-bit **functions** . Luby and Rackoff (1988) showed that 3 and 4 round Feistel networks require Omega (2/sup n/2/) queries to distinguish with theta (1) probability from truly random. We show that these bounds are tight by showing that these networks are susceptible various types of birthday attacks using O(2/sup n/2/) queries. (27 Refs)
Subfile: B C
Descriptors: cryptography; probability; random **functions**
Identifiers: birthday attacks; length-doubling transformations; cryptographic primitives; pseudorandom **functions** ; **hashing functions** ; non-reversible construction; Benes network; n-bit to n-bit random **function** ; 2n-bit to 2n-bit **function** ; truly random **function** ; unlimited computing power; Feistel networks
Class Codes: B6120B (Codes); B0240Z (Other topics in statistics); C6130S (Data security); C1140Z (Other topics in statistics)

17/5/7 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

05625710 INSPEC Abstract Number: B9404-6120B-070, C9404-6130S-046
Title: Interactive hashing **simplifies zero-knowledge protocol design**
Author(s): Ostrovsky, R.; **Venkatesan, R.** ; Moti Yung
Author Affiliation: Div. of Comput. Sci., California Univ., Berkeley, CA, USA
p.267-73
Editor(s): Helleseth, T.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1994 Country of Publication: West Germany x+465 pp.
ISBN: 3 540 57600 2
Conference Title: Proceedings of Advances in Cryptology - EUROCRYPT '93
Conference Date: 23-27 May 1993 Conference Location: Lofthus, Norway
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Often the core difficulty in designing zero-knowledge protocols arises from having to consider every possible cheating verifier trying to extract additional information. We consider a compiler which transforms protocols proven secure only with respect to the honest verifier into protocols which are secure against any (even cheating) verifier. Such a compiler, which preserves the zero-knowledge property of a statistically or computationally secure protocol was first proposed by M. Bellare et al (1990) based on discrete logarithm problem. We show how such a compiler could be constructed based on any one-way permutation using our recent method of interactive **hashing** . This applies to both statistically and computationally secure protocols, preserving their respective security. Our result allows us to utilize DES-like permutations for such a compiler. (21 Refs)
Subfile: B C
Descriptors: cryptography; file organisation; **program** compilers; protocols
Identifiers: interactive **hashing** ; zero-knowledge protocol design; compiler; computationally secure protocol; statistically secure protocol; discrete logarithm problem; one-way permutation
Class Codes: B6120B (Codes); B6150M (Protocols); B6210L (Computer communications); C6130S (Data security); C5640 (Protocols); C6150C (Compilers, interpreters and other processors); C6120 (File organisation)

17/5/8 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

07490406 Genuine Article#: BM51F Number of References: 38
Title: New constructions for secure hash functions **(Extended abstract)**
Author(s): Aiello W (REPRINT) ; Haber S; **Venkatesan R**
Corporate Source: BELLCORE,/MORRISTOWN//NJ/07960 (REPRINT); MICROSOFT RES,/REDMOND//WA/
, 1998, V1372, P150-167
ISSN: 0302-9743 Publication date: 19980000
Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, W-1000 BERLIN 33, GERMANYLECTURE NOTES IN COMPUTER SCIENCE
Series: LECTURE NOTES IN COMPUTER SCIENCE
Language: English Document Type: ARTICLE
Geographic Location: USA
Journal Subject Category: COMPUTER SCIENCE, THEORY & METHODS
Abstract: We present new, efficient and practical schemes for construction of collision-resistant **hash functions** , and analyze some simple methods for combining existing **hash - function** designs so as to enhance their security.

In our new constructions, we first map the input to a slightly longer string using a primitive we introduce called secure stretch **functions** . These are length-increasing almost surely injective one-way **functions** that sufficiently randomize their inputs so that it is hard for an adversary to force the outputs to fall into a target set. Then we apply a compression **function** to the output of the stretch **function** . We analyze the security of these constructions under different types of assumptions on both stretch and compression **functions** . These assumptions combine random- **function** models, intractability of certain ''biasing'' tasks, and the degeneracy structure of compression **functions** . The use of stretching seems to allow reduced requirements on the compression **function** , and may be of independent interest.

These constructions allow one to use popular and efficient primitives such as **MD5** , **SHA** -1, and RIPEMD that may exhibit weaknesses as collision-resistant **functions** . But no attacks are currently known on their one-way and randomizing properties, when they are used as stretch **functions** as in our constructions. There are several collision-resistant **hash functions** based on DEs for which there are no known effective attacks, but which are too slow for most practical **applications** . Our use of stretch **functions** enable us to base our compression **function** on DEs so that the resulting **hash function** achieves practical speeds: a test implementation runs at 40% of the speed of **MD5** .

We also suggest some imperfect random-oracle models, showing how to build better primitives from given imperfect ones. In this vein, we also analyze how to defend against a collision-finding adversary for a given primitive by building ''independent'' primitives.
Cited References:
US 4908861, 1990, BRACHTL BO
*NAT I STAND TECHN, 1994, V1801, NIST FED INF PROC ST
*SUR TECHN INC, 1995, ANSW FREQ ASK QUEST
AIELLO W, 1996, V1070, P307, LECT NOTES COMPUT SC
ANDERSON R, 1996, V1039, LECT NOTES COMPUTER
BOSELAERS A, 1996, V1109, P298, LECT NOTES COMPUTER
BOSSELAERS A, 1995, V1007, PCH3, LECT NOTES COMPUTER
BRASSARD G, 1991, V537, P94, LECT NOTES COMPUT SC
COPPERSMITH D, 1986, V218, P14, LECT NOTES COMPUTER
DAMGARD I, 1988, V435, P416, LECT NOTES COMPUTER
DAMGARD I, 1988, V304, P203, LECTURE NOTES COMPUT
DOBBERTIN H, 1996, V2, CRYTOBYTES

DOBBERTIN H, IN PRESS LECT NOTES
DOBBERTIN H, 1997, V10, P51, J CRYPTOL
DOBBERTIN H, 1996, V1039, P53, LECT NOTES COMPUTER
DOBBERTIN H, 1996, V1039, P71, LECT NOTES COMPUTER
DOBBERTIN H, 1996, RUMP SESS EUR 96
GOLDREICH O, 9609 THEOR CRYPT LIB
KNUDSEN L, 1997, V1294, P485, LECT NOTES COMPUTER
MATYAS SM, 1985, V27, P5658, IBM TECHNICAL DISCLO
MENEZES A, 1997, HDB APPLC RYPTOGRAPH
MERKLE RC, 1981, V24, P465, COMMUN ACM
MERKLE RC, 1990, V3, P43, J CRYPTOLOGY
MERKLE RC, 1990, V435, P428, LECTURE NOTES COMPUT
MERKLE RC, 1980, P122, P 1980 S SEC PRIV IE
MEYER CH, 1988, P111, SECURICOM 88
MIYAGUCHI S, 1990, V2, P128, NTT REVIEW
NAOR M, 1989, P33, P 21 S THEOR COMP AC
PEINADO M, 1997, LECT NOTES COMPUTER
PRENEEL B, 1997, COMMUNICATION
PRENEEL B, 1991, V773, P368, LECT NOTES COMPUTER
PRENEEL B, 1993, P183, P 1 ACM C COMP COMM
PRENEEL B, 1993, THESIS KATHOLIEKE U
RABIN MO, 1978, P155, F SECURE COMPUTATION
RIJMEN V, 1995, V1008, P242, LECT NOTES COMPUTER
RIVEST R, 1992, MD5 MESSAGE DIGEST A
RIVEST RL, 1991, V537, P303, LECT NOTES COMPUT SC
VANOORSCHOT P, 1994, P210, P 2 ACM C COMP COMM

17/5/9 (Item 2 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

05828352 Genuine Article#: BH79M Number of References: 27
Title: Foiling birthday attacks in length-doubling transformations - Benes: A non-reversible alternative to Feistel
Author(s): Aiello W (REPRINT) ; **Venkatesan R**
Corporate Source: BELL COMMUN RES INC,MATH & CRYPTOG RES GRP, 445 SOUTH S/MORRISTOWN//NJ/07960 (REPRINT)
, 1996, V1070, P307-320
ISSN: 0302-9743 Publication date: 19960000
Publisher: SPRINGER-VERLAG BERLIN, HEIDELBERGER PLATZ 3, W-1000 BERLIN 33, GERMANYLECTURE NOTES IN COMPUTER SCIENCE
Series: LECTURE NOTES IN COMPUTER SCIENCE
Language: English Document Type: ARTICLE
Geographic Location: USA
Journal Subject Category: COMPUTER SCIENCE, THEORY & METHODS
Abstract: For many cryptographic primitives, e.g., **hashing** and pseudorandom **functions** & generators, doubling the output length is useful even if the doubling transformation is not reversible. For these cases, me present a non-reversible construction based on a Benes network, as an alternative to the traditional Feistel construction (which is the basis of DES).

Assuming that a given primitive behaves like an n-bit to n-bit random **function** ,;we present a length-doubling scheme that yields a an-bit to an-bit **function** that provably requires Omega(2(n)) queries to distinguish with Theta(I) probability from a truly random **function** of that length. This is true even if the adversary is of unlimited computing power and is allowed to query the **function** adaptively Our construction is minimal in the sense that omitting any **operation** makes the resulting network susceptible to birthday attacks using O(2(n/2)) queries.

Feistel networks also use truly random n-bit **functions** to achieve 2n-bit **functions** . Luby and Rackoff [16] showed that 3 and 4 round Feistel networks require Omega(2(n/2)) queries to distinguish with O(I) probability from truly random. We show that these bounds are tight by showing that these networks are susceptible various types of birthday attacks using O(2(n/2)) queries.
Identifiers--KeyWord Plus(R): CONSTRUCT
Cited References:
BELLARE M, 1994, ADV CRYPTOLOGY CRYPT
BELLARE M, UNPUB KEYING MD5 MES
BIHAM E, 1992, ADV CRYPTOLOGY CRYPT
BIHAM E, 1991, ADV CRYPTOLOGY EUROC
BIHAM E, 1993, DIFFERENTIAL CRYPTAN
BLUM M, 1984, V13, P850, SIAM J COMPUT
COPPERSMITH D, 1986, ADV CRYPTOLOGY CRYPT
DAMGARD I, 1989, ADV CRYPTOLOGY CRYPT
DAVIES D, 1989, SECURITY COMPUTER NE
DOBBERTIN H, 1996, IN PRESS FAST SOFTWA
GOLDREICH O, 1986, V33, P792, J ASSOC COMPUT MACH
HASTAD J, 1989, P ACM S THEOR COMP
LANGFORD S, 1994, DIFFERENTIAL LINEAR
LEVIN L, 1985, P ACM S THEOR COMP
LUBY M, IN PRESS PSEUDORANDO
LUBY M, 1988, V17, P373, SIAM J COMPUT
MATSUI M, 1994, ADV CRYPTOLOGY CRYPT
MAURER U, 1992, ADV CRYPTOLOGY EUROC
MERKLE R, 1989, ADV CRYPTOLOGY CRYPT
MERKLE RC, 1990, V3, P43, J CRYPTOLOGY
PRENEEL B, 1995, ADV CRYPTOLOGY CRYPT
PRENEEL B, 1993, THESIS KATHOLIEKE U

SHOUP V, 1995, COMMUNICATION
VANOORSCHOT P, 1994, P 2 ACM C COMP COMMU
WYNER A, 1975, V54, BELL SYSTEM TECHNICA
YAO A, 1982, P IEEE S FDN COMP SC
ZHANG Y, 1989, ADV CRYPTOLOGY CRYPT

```
Set     Items   Description
S1         65   AU=JAKUBOWSKI M?
S2        143   AU=VENKATESAN R?
S3        172   S1 OR S2
S4         67   S3 AND IC=G06F
S5         67   IDPAT (sorted in duplicate/non-duplicate order)
S6         42   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200622
         (c) 2006  Thomson Derwent
File 349:PCT FULLTEXT 1979-2006/UB=20060330,UT=20060323
         (c) 2006 WIPO/Univentio
File 348:EUROPEAN PATENTS 1978-2006/ 200613
         (c) 2006 European Patent Office
```

```
Set     Items   Description
S1         65   AU=JAKUBOWSKI M?
S2        143   AU=VENKATESAN R?
S3        172   S1 OR S2
S4         67   S3 AND IC=G06F
S5         67   IDPAT (sorted in duplicate/non-duplicate order)
S6         42   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Dec 1976-2005/Dec(Updated 060404)
         (c) 2006 JPO & JAPIO
File 350:Derwent WPIX 1963-2006/UD,UM &UP=200622
         (c) 2006  Thomson Derwent
File 349:PCT FULLTEXT 1979-2006/UB=20060330,UT=20060323
         (c) 2006 WIPO/Univentio
File 348:EUROPEAN PATENTS 1978-2006/ 200613
         (c) 2006 European Patent Office
```

6/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017386548 **Image available**
WPI Acc No: 2005-710203/200573
Related WPI Acc No: 2004-794066; 2005-010915
XRPX Acc No: N05-582991

Program profile information reuse system has processing engine to process portions of two versions of program to produce two values using set of information at desired fuzziness level

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MCFARLING S A; PIERCE K B; **VENKATESAN R** ; WANG Z
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6954747	B1	20051011	US 2000712063	A	20001114	200573	B

Priority Applications (No Type Date): US 2000712063 A 20001114
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6954747	B1		13	G06F-017/00	

Abstract (Basic): US 6954747 B1

NOVELTY - The program profile information reuse system (200) has a propagator (208) to propagate profile information when a match between first and second values is found using a comparator (206). Processing engine (204) processes a portion of first version of a program to produce the first value and a portion of a second version of the program to produce the second value, using a set of information at a desired fuzziness.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a method for comparing versions of a program in a binary format.

USE - For reusing profile information of a program.

ADVANTAGE - Allows profile information to be reused by various versions of a program. Allows more time to collect profile information not found in the reused file information.

DESCRIPTION OF DRAWING(S) - The figure is a system diagram that shows the engine for comparing two versions of a program.

Program profile information reuse system (200)
Processing engine (204)
Comparator (206)
Propagator (208)
pp; 13 DwgNo 2/9

Title Terms: PROGRAM; PROFILE; INFORMATION; REUSE; SYSTEM; PROCESS; ENGINE; PROCESS; PORTION; TWO; VERSION; PROGRAM; PRODUCE; TWO; VALUE; SET; INFORMATION; LEVEL
Derwent Class: T01
International Patent Class (Main): **G06F-017/00**
International Patent Class (Additional): **G06F-012/00** ; **G06F-015/18**
File Segment: EPI

6/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017368310 **Image available**
WPI Acc No: 2005-691959/200572
XRPX Acc No: N05-567785

Stream cipher designing method for secure digital communication in networked computing environment, involves rotating storage units serially, when threshold values corresponding to output pairing results are reached

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MIRONOV I; **VENKATESAN R** ; MIRONOV L
Number of Countries: 043 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1583278	A1	20051005	EP 2005102396	A	20050324	200572	B
CA 2497935	A1	20050930	CA 2497935	A	20050222	200572	
JP 2005295507	A	20051020	JP 200533533	A	20050209	200572	
US 20050220302	A1	20051006	US 2004815572	A	20040331	200572	
BR 200500539	A	20051101	BR 2005539	A	20050218	200574	
CN 1677917	A	20051005	CN 200552841	A	20050225	200606	
AU 2005200388	A1	20051020	AU 2005200388	A	20050131	200615	
MX 2005002553	A1	20051001	MX 20052553	A	20050304	200620	

Priority Applications (No Type Date): US 2004815572 A 20040331
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1583278	A1		19	H04L-009/18	
Designated States (Regional): AL AT BA BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU					
CA 2497935	A1	E		H04L-009/18	
JP 2005295507	A		20	H04L-009/22	
US 20050220302	A1			H04L-009/00	
BR 200500539	A			G09C-001/04	
CN 1677917	A			H04L-009/00	
AU 2005200388	A1			H04L-009/18	
MX 2005002553	A1			G06F-003/00	

Abstract (Basic): EP 1583278 A1

NOVELTY - The method involves storing results provided by a stream cipher output rule, sequentially in first, second and third storage units implement in a memory device. The results obtained by pairing individual values from first and third storage units which are active at any given time, are output. The storage units are serially rotated when threshold values corresponding to the output results are reached.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) stream cipher designing system; and

(2) computer-readable medium storing stream cipher designing program.

USE - For designing stream cipher using revolving buffers in networked computing environment including communication media such as wired or direct-wired connection, wireless media such as acoustic media, radio frequency (RF) media, wireless fidelity (WiFi) network, cellular network and Bluetooth network, for providing secure digital communication of information such as user's bank account, medical data and other private/sensitive information.

ADVANTAGE - Effectively produces sequences with improved statistical properties, such that the sequences are readily analyzed using algebraic techniques.

DESCRIPTION OF DRAWING(S) - The figure shows a flow chart explaining the stream cipher designing process.

pp; 19 DwgNo 6/7

Title Terms: STREAM; CIPHER; DESIGN; METHOD; SECURE; DIGITAL; COMMUNICATE;

COMPUTATION; ENVIRONMENT; ROTATING; STORAGE; UNIT; SERIAL; THRESHOLD; VALUE; CORRESPOND; OUTPUT; PAIR; RESULT; REACH

Derwent Class: T01; W01

International Patent Class (Main): **G06F-003/00** ; G09C-001/04; H04L-009/00; H04L-009/18; H04L-009/22

File Segment: EPI

6/5/3 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017351778 **Image available**
WPI Acc No: 2005-675420/200569
XRPX Acc No: N05-554049
Front page inconsistent with claims, abstract based on front page and disclosure. Patent office notified - message authentication code provision based on unimodular matrices
Patent Assignee: CARY M C (CARY-I); VENKATESAN R (VENK-I)
Inventor: CARY M C; **VENKATESAN R**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20050210260	A1	20050922	US 2004803108	A	20040317	200569	B

Priority Applications (No Type Date): US 2004803108 A 20040317
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050210260	A1		30	G06F-012/00	

Abstract (Basic): US 20050210260 A1
NOVELTY - The message authentication code provision method involves providing length controllable hash values comprised of vector pairs that can be processed as one instruction in single instruction, multiple data (SIMD) equipped computational processor where the vector pair is treated as a double word.
USE - For providing message authentication code based on unimodular matrices for document indexing and retrieval, document integrity checking for database and secure networks and web search and server applications and for other data protection scheme such as checksumming critical data e.g. airplane flight control information.
ADVANTAGE - Provides universal hash function with reversible properties and high speed performance.
DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram of method of facilitating data transformation.
pp; 30 DwgNo 7/14
Title Terms: FRONT; PAGE; CLAIM; ABSTRACT; BASED; FRONT; PAGE; DISCLOSE; PATENT; OFFICE; NOTIFICATION; MESSAGE; AUTHENTICITY; CODE; PROVISION; BASED; MATRIX
Derwent Class: T01
International Patent Class (Main): **G06F-012/00**
File Segment: EPI

6/5/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017257497 **Image available**
WPI Acc No: 2005-581120/200559
XRPX Acc No: N05-476786

Digital data e.g. movie, desynchronized fingerprinting method, involves selecting embedding regions in data for embedding fingerprints at each regions to produce desynchronized fingerprinted data

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: KUCUKGOZ M; MIHCAK M K; **VENKATESAN R**
Number of Countries: 043 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20050175224	A1	20050811	US 2004777915	A	20040211	200559	B
CA 2491826	A1	20050811	CA 2491826	A	20050110	200560	
JP 2005227756	A	20050825	JP 20054479	A	20050111	200560	
EP 1569063	A2	20050831	EP 200430841	A	20041227	200561	
AU 2004240154	A1	20050825	AU 2004240154	A	20041215	200562	
BR 200405606	A	20050927	BR 20045606	A	20041217	200565	
CN 1655500	A	20050817	CN 200461568	A	20041227	200572	
MX 2005000524	A1	20051001	MX 2005524	A	20050111	200620	

Priority Applications (No Type Date): US 2004777915 A 20040211
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050175224	A1		21	H04N-007/167	
CA 2491826	A1	E		G06F-012/14	
JP 2005227756	A		27	G09C-005/00	
EP 1569063	A2	E		G06F-001/00	
Designated States (Regional): AL AT BA BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU					
AU 2004240154	A1			G06F-012/14	
BR 200405606	A			G06K-009/00	
CN 1655500	A			H04L-009/14	
MX 2005000524	A1			G06K-009/00	

Abstract (Basic): US 20050175224 A1

NOVELTY - The method involves selecting embedding regions in a digital data for embedding fingerprints and selecting desynchronization regions for desynchronizing copies of the data from each other. Random desynchronization is performed for each of the desynchronization regions to randomly vary a width of each desynchronization region. The fingerprints are embedded at each embedded regions to produce desynchronized fingerprinted data.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(A) a computer-readable medium having computer-executable instructions for performing the computer-implemented method

(B) a process for detecting and extracting fingerprint from digital data

(C) a desynchronized fingerprinting system for desynchronized fingerprinting of copies of an original digital multimedia product.

USE - Used for desynchronized fingerprinting of a digital data e.g. movie and audio.

ADVANTAGE - The method enables identification of large number of collaborators without the use of fingerprinting codes and provides strong deterrent to illegal copying.

DESCRIPTION OF DRAWING(S) - The drawing shows a general flow diagram of a desynchronized embedding process of a desynchronized fingerprinting method.

pp; 21 DwgNo 3/9

Title Terms: DIGITAL; DATA; MOVIE; FINGERPRINT; METHOD; SELECT; EMBED; REGION; DATA; EMBED; FINGERPRINT; REGION; PRODUCE; DATA

Derwent Class: T01; W04
International Patent Class (Main): **G06F-001/00** ; **G06F-012/14** ;
G06K-009/00; G09C-005/00; H04L-009/14; H04N-007/167
International Patent Class (Additional): **G06F-017/60** ; G06T-001/00;
H04L-009/32; H04N-001/387
File Segment: EPI

6/5/5 (Item 5 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017229678 **Image available**
WPI Acc No: 2005-553300/200556
XRPX Acc No: N05-453535
Processor readable medium for e.g. personal computer, has instructions **for calculating and quantizing rational statistics e.g. semi-global characteristics, of regions, where digital good is water marked based on statistics**
Patent Assignee: MICROSOFT CORP (MICT)
Inventor: LIU T; MIHCAK M K; **VENKATESAN R**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20050165690	A1	20050728	US 2004764345	A	20040123	200556	B

Priority Applications (No Type Date): US 2004764345 A 20040123
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050165690	A1		15	G06F-017/60	

Abstract (Basic): US 20050165690 A1
NOVELTY - The medium has instructions for obtaining a digital good e.g. audio signal, by a goods obtainer (210), and partitioning the good into a set of regions by a partitioner (230). The good is received by a transformer that puts the good in a canonical form. Rational statistics e.g. semi-global characteristics, of the regions are calculated and quantized, and the digital good is water marked based on the statistics of the regions.
DETAILED DESCRIPTION - An INDEPENDENT CLAIMS is also included for a watermark embedding system comprising a partitioner to segment a digital good into regions.
USE - Used for water marking digital good e.g. audio signal and digital image, in a computing system e.g. personal computer, server computer, laptop device, multiprocessor system, microprocessor- based system, programmable consumer electronics, wireless phone, network personal computer, minicomputer and mainframe computer.
ADVANTAGE - The rational statistics e.g. semi-global characteristics, of the regions are calculated and quantized, and digital good is water marked based on the statistics, thus minimizing perceptual distortion between watermarked data and data of the digital goods.
DESCRIPTION OF DRAWING(S) - The drawing shows a schematic block diagram watermark embedding system.
Audio signal (205)
Goods obtainer (210)
Transformer (220)
Partitioner (230)
Region statistics calculator (240)
pp; 15 DwgNo 2/7
Title Terms: PROCESSOR; READ; MEDIUM; PERSON; COMPUTER; INSTRUCTION; CALCULATE; QUATERNISED; RATIONAL; STATISTICAL; SEMI; GLOBE; CHARACTERISTIC; REGION; DIGITAL; WATER; MARK; BASED; STATISTICAL
Derwent Class: T01
International Patent Class (Main): **G06F-017/60**
File Segment: EPI

6/5/6 (Item 6 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017196947 **Image available**
WPI Acc No: 2005-520574/200553
Related WPI Acc No: 2005-513778
XRPX Acc No: N05-425127

Processor-readable medium storing digital goods representation program, comprises codes to represent digital goods e.g. audio clips in defined representation domain, based on matrix invariances including singular value decomposition

Patent Assignee: MICROSOFT CORP (MICT); KOZAT S S (KOZA-I); MIHCAK M K (MIHC-I); VENKATESAN R (VENK-I)
Inventor: KOZAT S S; MIHCAK M K; **VENKATESAN R**
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20050149727	A1	20050707	US 2004752268	A	20040106	200553	B
JP 2005196744	A	20050721	JP 2004353231	A	20041206	200553	

Priority Applications (No Type Date): US 2004752268 A 20040106
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20050149727	A1		13	H04L-009/00	
JP 2005196744	A		21	G06F-012/14	

Abstract (Basic): US 20050149727 A1

NOVELTY - The digital goods such as audio signals/digital images are represented in a defined representation domain, based on matrix invariances including singular value decomposition (SVD).

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) computing device;
(2) computer; and
(3) content distribution system.

USE - For representing digital goods including image, audio clips, video, multimedia, software and database, distributed to consumer through internet, in defined representation domain, for adversarial and non-adversarial applications and in certification applications.

ADVANTAGE - Enables considering the digital goods as two dimensional surfaces in a three dimensional space, by using singular value decomposition (SVD).

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart explaining the digital goods representation method.

pp; 13 DwgNo 1/3

Title Terms: PROCESSOR; READ; MEDIUM; STORAGE; DIGITAL; GOODS; REPRESENT; PROGRAM; COMPRISE; CODE; REPRESENT; DIGITAL; GOODS; AUDIO; CLIP; DEFINE; REPRESENT; DOMAIN; BASED; MATRIX; SINGULAR; VALUE; DECOMPOSE
Derwent Class: T01; W02; W04
International Patent Class (Main): **G06F-012/14** ; H04L-009/00
International Patent Class (Additional): **G06F-017/30** ; **G06F-017/60** ; H04N-001/387
File Segment: EPI

6/5/7 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017190151 **Image available**
WPI Acc No: 2005-513778/200553
Related WPI Acc No: 2005-520574
XRPX Acc No: N05-419353

Processor-readable medium storing programs for hashing techniques, includes instructions for representing digital goods in defined representation domain based upon matrix invariance

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: KOZAT S S; MIHCAK M K; VENKATESEN R; **VENKATESAN R**
Number of Countries: 039 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1553476	A2	20050713	EP 200427449	A	20041118	200553	B
AU 2004237806	A1	20050721	AU 2004237806	A	20041208	200553	
CA 2487151	A1	20050706	CA 2487151	A	20041108	200553	
BR 200405021	A	20050920	BR 20045021	A	20041111	200566	
CN 1638328	A	20050713	CN 20041100617	A	20041201	200576	

Priority Applications (No Type Date): US 2004752268 A 20040106
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1553476	A2		16	G06F-001/00	
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR YU					
AU 2004237806	A1			G06F-017/16	
CA 2487151	A1	E		G06F-017/00	
BR 200405021	A			H04L-009/32	
CN 1638328	A			H04L-009/22	

Abstract (Basic): EP 1553476 A2

NOVELTY - Processor readable medium stores instructions for representing digital audio clip, digital video, database and a software image in a defined representation domain based on the matrix invariance.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) computing device;

(2) computer for representing digital goods in defined representation domain;

(3) method for representing digital goods in defined representation domain; and

(4) system for representing digital goods in defined representation domain.

USE - For storing hashing techniques used in database management, querying, cryptography, content recognition, water marking, content based key generation and synchronization of audio and video streams. Also used to search the web for digital goods suspected of having being pirated, to generate secret keys based upon the content of signal.

ADVANTAGE - Produces new representation of digital goods in a new defined representation domain.

DESCRIPTION OF DRAWING(S) - The figure shows a schematic view of the computing environment.

computing environment (300)
computer (302)
magnetic disk drive (318)
removable magnetic disk (320)
optical disk drive (322)
removable optical disk (324)

pp; 16 DwgNo 3/3

Title Terms: PROCESSOR; READ; MEDIUM; STORAGE; PROGRAM; HASH; TECHNIQUE; INSTRUCTION; REPRESENT; DIGITAL; GOODS; DEFINE; REPRESENT; DOMAIN; BASED;

MATRIX; INVARIANT
Derwent Class: T01
International Patent Class (Main): **G06F-001/00** ; **G06F-017/00** ; **G06F-017/16** ; H04L-009/22; H04L-009/32
International Patent Class (Additional): **G06F-012/14** ; **G06F-017/30** ; G06T-001/00
File Segment: EPI

6/5/8 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

017023605 **Image available**
WPI Acc No: 2005-347922/200536
XRPX Acc No: N05-284182

Isogenies usage method in cryptosystem, involves generating isogeny that maps several points of two elliptic curves, and encrypting/decrypting message using corresponding public keys based on generated isogeny

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: JAO D Y; **VENKATESAN R**
Number of Countries: 043 Number of Patents: 011
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 1528705	A1	20050504	EP 200418957	A	20040810	200536	B
CA 2483486	A1	20050503	CA 2483486	A	20041001	200536	
US 20050094806	A1	20050505	US 2003517142	P	20031103	200536	
			US 2004816083	A	20040331		
AU 2004218638	A1	20050519	AU 2004218638	A	20041006	200537	
JP 2005141200	A	20050602	JP 2004290612	A	20041001	200537	
NO 200404028	A	20050504	NO 20044028	A	20040924	200537	
BR 200404122	A	20050621	BR 20044122	A	20040920	200542	
SG 111191	A1	20050530	SG 20044557	A	20040810	200544	
CN 1614922	A	20050511	CN 200468590	A	20040827	200558	
MX 2004010155	A1	20050501	MX 200410155	A	20041015	200572	
NZ 535698	A	20060224	NZ 535698	A	20041001	200620	

Priority Applications (No Type Date): US 2004816083 A 20040331; US 2003517142 P 20031103
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1528705	A1	E	18	H04L-009/30	
Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IT LI LT LU LV MC MK NL PL PT RO SE SI SK TR					
CA 2483486	A1	E		H04L-009/30	
US 20050094806	A1			H04K-001/00	Provisional application US 2003517142
AU 2004218638	A1			H04L-009/30	
JP 2005141200	A		27	G09C-001/00	
NO 200404028	A			H04L-009/32	
BR 200404122	A			H04L-009/30	
SG 111191	A1			H04L-009/30	
CN 1614922	A			H04L-009/30	
MX 2004010155	A1			H03M-013/07	
NZ 535698	A			H04L-009/28	

Abstract (Basic): EP 1528705 A1

NOVELTY - An isogeny that maps several points of two elliptic curves, is generated. A public key corresponding to the generated isogeny is published. A message is encrypted and decrypted using encryption and decryption key corresponding to the isogeny, respectively.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) isogenies usage system; and

(2) computer-readable medium storing isogenies usage program.

USE - For using isogenies for cryptosystem used for providing secure digital communication of remotely accessed bank accounts, medical data or other private and sensitive information, through network such as acoustic network, radio frequency (RF) network, infrared (IR) network, wireless fidelity (WiFi) network, cellular network. Also in applications such as blind signatures, hierarchical systems.

ADVANTAGE - Allows the public key encryption system to provide additional security through aggregate verification.

DESCRIPTION OF DRAWING(S) - The figure shows a flow diagram explaining the usage of isogenies in cryptosystem.

pp; 18 DwgNo 1/6

Title Terms: METHOD; GENERATE; MAP; POINT; TWO; ELLIPSE; CURVE; MESSAGE; CORRESPOND; PUBLIC; KEY; BASED; GENERATE

Derwent Class: T01; W01

International Patent Class (Main): G09C-001/00; H03M-013/07; H04K-001/00; H04L-009/28; H04L-009/30; H04L-009/32

International Patent Class (Additional): **G06F-007/72**

File Segment: EPI

6/5/9 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016755648 **Image available**
WPI Acc No: 2005-079926/200509
Related WPI Acc No: 2003-776889
XRPX Acc No: N05-070291

Text content recognition method in computer involves text-sifting contents of text to remove punctuation and non-essential words and determining hash value based on sifted subtext

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MALKIN M T; **VENKATESAN R**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040268220	A1	20041230	US 2001843255	A	20010424	200509	B
			US 2004893769	A	20040716		

Priority Applications (No Type Date): US 2001843255 A 20010424; US 2004893769 A 20040716
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040268220	A1		20	G06F-017/00	Cont of application US 2001843255

Abstract (Basic): US 20040268220 A1

NOVELTY - The contents of a text are text-sifted to remove punctuation and other non-essential words and the text is put into a standard format. The subtext is extracted through a self-synchronized approach such as fixed length subtext extraction or variable length subtext extraction. The extracted subtext is arranged in a standard format. The hash value is determined based on the sifted subtext.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) computer;
(2) computer readable media;
(3) method for facilitating detection of textual similarity;
(4) method of manipulating content of text; and
(5) text recognition system.

USE - For facilitating recognition of content of text in e-books, electronic publishing ,electronic mail (e-mail), portable document format (pdf) documents, web pages and on-line newspaper in computer (claimed) such as personal computer (PC), server computer, hand-held or laptop computer, multiprocessor system, programmable consumer electronics, wireless telephone, general and special purpose appliances, application specific integrated circuit (ASIC), network personal computer (PC), minicomputer, mainframe computer and distributed computing environment.

ADVANTAGE - The content of the text-based work is categorized automatically in an accurate manner.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the recognizer of the text-based work.

text identification subsystem (100)

pp; 20 DwgNo 1/7

Title Terms: TEXT; CONTENT; RECOGNISE; METHOD; COMPUTER; TEXT; SIEVE; CONTENT; TEXT; REMOVE; PUNCTUATION; NON; ESSENTIAL; WORD; DETERMINE; HASH ; VALUE; BASED; SIEVE
Derwent Class: T01
International Patent Class (Main): **G06F-017/00**
File Segment: EPI

6/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016686634 **Image available**
WPI Acc No: 2005-010915/200501
Related WPI Acc No: 2004-794066; 2005-710203
XRPX Acc No: N05-008746

Program profile information reuse system processes two different program versions at desired fuzziness level, defines match between program contents, and propagates profile information for reuse by various program versions

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MCFARLING S A; PIERCE K B; **VENKATESAN R** ; WANG Z
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040230957	A1	20041118	US 2000712063	A	20001114	200501	B
			US 2004874676	A	20040624		

Priority Applications (No Type Date): US 2000712063 A 20001114; US 2004874676 A 20040624
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040230957	A1		15	G06F-009/44	Cont of application US 2000712063

Abstract (Basic): US 20040230957 A1

NOVELTY - A processing engine processes the two different versions of the program, at desired fuzziness level, and generates two output values. When the two values are equal, the comparator defines a match between the content of the two versions, and a propagator propagates the profile information for reuse by various versions of the program.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) program versions comparison method;

(2) computer readable medium storing program versions comparison program;

(3) program data comparison method;

(4) program code comparison method; and

(5) method for hashing code to compare program versions.

USE - For reusing profile information of program, for different versions of program.

ADVANTAGE - Enables reusing the profile information of the program, thereby reduces the time required for collecting the desired profile information, reduces the size and complexity of the program, and eliminates the need for generating quality profile information for program improvement.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram program profile information reuse system.

pp; 15 DwgNo 1/8

Title Terms: PROGRAM; PROFILE; INFORMATION; REUSE; SYSTEM; PROCESS; TWO; PROGRAM; VERSION; LEVEL; DEFINE; MATCH; PROGRAM; CONTENT; PROPAGATE; PROFILE; INFORMATION; REUSE; VARIOUS; PROGRAM; VERSION
Derwent Class: T01
International Patent Class (Main): **G06F-009/44**
File Segment: EPI

6/5/11 (Item 11 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016635353 **Image available**
WPI Acc No: 2004-794066/200478
Related WPI Acc No: 2005-010915; 2005-710203
XRPX Acc No: N04-625772

Program profile information reusing system, has processing engine that processes two portions of versions of program, to produce respective values, where engine uses set of information at desired fuzziness level to form values

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MCFARLING S A; PIERCE K B; **VENKATESAN R** ; WANG Z
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040210885	A1	20041021	US 2000712063	A	20001114	200478	B
			US 2004842613	A	20040510		

Priority Applications (No Type Date): US 2000712063 A 20001114; US 2004842613 A 20040510
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040210885	A1		15	G06F-009/45	Div ex application US 2000712063

Abstract (Basic): US 20040210885 A1

NOVELTY - The system has a propagator to propagate profile information when a comparator defines a match between two values. A processing engine processes a portion of a version (102) of a program to produce one of the values and another portion of another version (112) of the program to produce another value, where the processing engine uses a set of information at a desired fuzziness level to produce the values.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(A) a method for comparing versions of a program in binary format

(B) a computer readable medium having instructions stored for causing a computer to perform a method for comparing versions of a program in binary format

(C) a method for hashing code to compare versions.

USE - Used for reusing profile information of a program.

ADVANTAGE - The method analyzes the program without referring to a source code of the program, thereby collecting profile information in a desired amount of time, and hence providing effective acceptance level of the programs in the market place.

DESCRIPTION OF DRAWING(S) - The drawing shows a system diagram that depicts reusing profile information.

versions (102,112)
Profiles (106,116)
Conversions (118)
pp; 15 DwgNo 1/9

Title Terms: PROGRAM; PROFILE; INFORMATION; REUSE; SYSTEM; PROCESS; ENGINE; PROCESS; TWO; PORTION; VERSION; PROGRAM; PRODUCE; RESPECTIVE; VALUE; ENGINE; SET; INFORMATION; LEVEL; FORM; VALUE
Derwent Class: T01
International Patent Class (Main): **G06F-009/45**
File Segment: EPI

6/5/12 (Item 12 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015940512 **Image available**
WPI Acc No: 2004-098353/200410
XRPX Acc No: N04-078440

Opaque type libraries provision system for secure data protection of variables in personal computer, substitutes selected variable obfuscation function for each declared secure variable

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: CHEN Y; **JAKUBOWSKI M H** ; **VENKATESAN R**

Number of Countries: 033 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20040003278	A1	20040101	US 2002185644	A	20020628	200410	B
EP 1376310	A2	20040102	EP 200314102	A	20030623	200410	
JP 2004038966	A	20040205	JP 2003178499	A	20030623	200411	

Priority Applications (No Type Date): US 2002185644 A 20020628
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040003278	A1		20	G06F-012/14	
EP 1376310	A2	E		G06F-001/00	
				Designated States (Regional): AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LT LU LV MC MK NL PT RO SE SI SK TR	
JP 2004038966	A		51	G06F-001/00	

Abstract (Basic): US 20040003278 A1

NOVELTY - An opaque type libraries (OTL) selection module selects one of the variable obfuscation functions for each declared secure variable and an OTL substitution module substitutes the selected function for each variable. An OTL type library database receiving queries from the OTL selection module, identifies the variable obfuscation functions applicable for variable type corresponding to the declared secure variables.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) method for providing secure and opaque type libraries; and

(2) computer program data product for providing secure and opaque type libraries.

USE - For providing secure opaque type libraries to automatically provide secure variables within programming module of personal computers (PCs), server computers, handheld or laptop devices, multiprocessor systems, microprocessor-based systems, programmable consumer electronics, network PCs, mini computers, mainframe computers, and distributed computing environments.

ADVANTAGE - Enables to provide secure data protection of variables within programming module efficiently.

DESCRIPTION OF DRAWING(S) - The figure shows illustrate a computing system to create secure variables.

computer (103)
source code (110)
OTL processing module (121)
compiler module (122)
linker module (123)
pp; 20 DwgNo 1/10

Title Terms: OPAQUE; TYPE; PROVISION; SYSTEM; SECURE; DATA; PROTECT; VARIABLE; PERSON; COMPUTER; SUBSTITUTE; SELECT; VARIABLE; FUNCTION; SECURE; VARIABLE
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/00** ; **G06F-012/14**
International Patent Class (Additional): **G06F-007/00** ; **G06F-009/44** ; **G06F-009/45** ; **G06F-011/30** ; **G06F-017/00** ; H04L-009/00; H04L-009/32

File Segment: EPI

6/5/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015460514 **Image available**
WPI Acc No: 2003-522656/200349
Related WPI Acc No: 2000-611744; 2000-647267; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2001-596397; 2002-279866; 2002-350656; 2002-392575; 2005-617252; 2005-701313
XRPX Acc No: N03-414746

Enforcement architecture has digital rights management which determines whether user has right to render requested digital content based on digital license stored for corresponding content

Patent Assignee: ABBURI R (ABBU-I); BELL J R C (BELL-I); BLINN A N (BLIN-I); ENGLAND P (ENGL-I); JAKUBOWSKI M H (JAKU-I); JONES T C (JONE-I); MANFERDELLI J L (MANF-I); PEINADO M (PEIN-I); VENKATESAN R (VENK-I); YU H Y (YUHY-I)
Inventor: ABBURI R; BELL J R C; BLINN A N; ENGLAND P; **JAKUBOWSKI M H** ; JONES T C; MANFERDELLI J L; PEINADO M; **VENKATESAN R** ; YU H Y
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20030078853	A1	20030424	US 99126614	P	19990327	200349 B
			US 99290363	A	19990412	
			US 2002208139	A	20020729	

Priority Applications (No Type Date): US 99126614 P 19990327; US 99290363 A 19990412; US 2002208139 A 20020729
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030078853	A1		37	G06F-017/60	Provisional application US 99126614
					Cont of application US 99290363

Abstract (Basic): US 20030078853 A1

NOVELTY - A computing device (14) stores digital license issued by license server (24) corresponding to the digital content (12). A digital rights management (DRM) which corresponds to user's rendering application, determines whether the user has right to render the requested content based on licenses stored for the corresponding content if not a license that provides such right is requested from a license server and issued.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for digital rights management implementation method.

USE - For enforcing rights in protected digital content such as digital audio, digital video, digital text, digital data, digital multimedia to user.

ADVANTAGE - The enforcement architecture provided allow controlled rendering or playing of arbitrary forms of digital content based on the license provided for corresponding content, thus preventing user of the computing device from making a copy of the content until allowed by the content server.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram to the enforcement architecture.

digital content (12)
computing device (14)
license server (24)
pp; 37 DwgNo 1/12

Title Terms: ARCHITECTURE; DIGITAL; MANAGEMENT; DETERMINE; USER; RIGHT; RENDER; REQUEST; DIGITAL; CONTENT; BASED; DIGITAL; LICENCE; STORAGE; CORRESPOND; CONTENT
Derwent Class: T01
International Patent Class (Main): **G06F-017/60**

File Segment: EPI

6/5/14 (Item 14 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014987944 **Image available**
WPI Acc No: 2003-048459/200305
XRPX Acc No: N03-038150

Computer implemented digital audio signal identification method involves deriving identical hash values for perceptually same digital signals and independent hash values for perceptually distinct digital signals

Patent Assignee: MICROSOFT CORP (MICT); MIHCAK M K (MIHC-I); VENKATESAN R (VENK-I)
Inventor: MIHCAK M K; **VENKATESAN R**
Number of Countries: 028 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 1253525	A2	20021030	EP 20026189	A	20020319	200305 B
US 20020184505	A1	20021205	US 2001843254	A	20010424	200305
JP 2003005771	A	20030108	JP 2002123172	A	20020424	200315
US 20050071377	A1	20050331	US 2001843254	A	20010424	200524
			US 2004980907	A	20041104	
US 20050076229	A1	20050407	US 2001843254	A	20010424	200525
			US 2004994498	A	20041122	
US 20050065974	A1	20050324	US 2001843254	A	20010424	200526
			US 2004980919	A	20041104	
US 20050066176	A1	20050324	US 2001843254	A	20010424	200526
			US 2004981165	A	20041104	
US 20050066177	A1	20050324	US 2001843254	A	20010424	200526
			US 2004980918	A	20041104	
US 20050084103	A1	20050421	US 2001843254	A	20010424	200528
			US 2004980917	A	20041104	
US 20050097312	A1	20050505	US 2001843254	A	20010424	200531
			US 200412968	A	20041215	
US 6971013	B2	20051129	US 2001843254	A	20010424	200578
			US 200412968	A	20041215	
US 6973574	B2	20051206	US 2001843254	A	20010424	200580

Priority Applications (No Type Date): US 2001843254 A 20010424; US 2004980907 A 20041104; US 2004994498 A 20041122; US 2004980919 A 20041104; US 2004981165 A 20041104; US 2004980918 A 20041104; US 2004980917 A 20041104; US 200412968 A 20041215
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1253525	A2	E	28	G06F-017/17	
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
US 20020184505	A1			H04L-009/00	
JP 2003005771	A		24	G10L-011/00	
US 20050071377	A1			G06F-017/00	Cont of application US 2001843254
US 20050076229	A1			H04L-009/00	Cont of application US 2001843254
US 20050065974	A1			G06F-017/00	Cont of application US 2001843254
US 20050066176	A1			H04L-009/00	Cont of application US 2001843254
US 20050066177	A1			H04L-009/00	Cont of application US 2001843254
US 20050084103	A1			H04L-009/00	Cont of application US 2001843254
US 20050097312	A1			G06F-007/00	Cont of application US 2001843254
US 6971013	B2			H04L-009/00	Cont of application US 2001843254
US 6973574	B2			H04L-009/00	

Abstract (Basic): EP 1253525 A2

NOVELTY - The hash value representative of the digital signal, is derived such that perceptually distinct digital signals have hash values that are approximately independent of one another and perceptually same digital signals have identical hash values.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Computer-readable medium storing digital audio signal identification program;
(2) Computer-implemented digital signal hashing method;
(3) Digital signal processing system; and
(4) Computer implemented digital signal recognition method.
USE - For identifying the digital audio signal using computer.
ADVANTAGE - Improves the recognition of audio content in the digital signal deriving identical hash values for perceptually same digital signal.
DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the audio digital signal recognizer.
pp; 28 DwgNo 1/9

Title Terms: COMPUTER; IMPLEMENT; DIGITAL; AUDIO; SIGNAL; IDENTIFY; METHOD; DERIVATIVE; IDENTICAL; HASH; VALUE; DIGITAL; SIGNAL; INDEPENDENT; HASH; VALUE; DISTINCT; DIGITAL; SIGNAL
Derwent Class: P86; T01; W04
International Patent Class (Main): **G06F-007/00** ; **G06F-017/00** ; **G06F-017/17** ; G10L-011/00; H04L-009/00
International Patent Class (Additional): **G06F-017/30** ; G06K-009/00; G10H-001/00; G10L-019/00; H04N-007/167
File Segment: EPI; EngPI

6/5/15 (Item 15 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014652361 **Image available**
WPI Acc No: 2002-473065/200251
XRPX Acc No: N02-373459

Delta generation method for program binaries, involves identifying unmatched blocks which are merged into source control flow graph representation so that source and target Control Flow Graph's (CFG's) are identical

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: SINHA S; **VENKATESAN R**

Number of Countries: 028 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 1205842	A2	20020515	EP 2001126979	A	20011113	200251 B
JP 2002169702	A	20020614	JP 2001349299	A	20011114	200254
US 20040225996	A1	20041111	US 2000713633	A	20001114	200475
			US 2004862554	A	20040607	

Priority Applications (No Type Date): US 2000713633 A 20001114; US 2004862554 A 20040607
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 1205842	A2	E	29	G06F-009/44	
	Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR				
JP 2002169702	A		23	G06F-011/00	
US 20040225996	A1			G06F-009/44	Cont of application US 2000713633

Abstract (Basic): EP 1205842 A2

NOVELTY - Control flow graph (CFG) representations of a source program (112) and a target program (122) are compared to identify matched and unmatched blocks. Edit operations that merge the unmatched blocks into the source representation, is determined so that source and target representations are identical. A delta (142) comprising the unmatched blocks and edit operations, is produced.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for :
(1) Computer readable medium for storing delta generation program;
(2) Block matching method;
(3) Patch data structure;
(4) Patch data structure transmission method;
(5) Source program patching method;
(6) Delta generator system;
(7) Computer readable medium storing data structure comprising generated delta;
(8) Computer readable medium storing block matching program;
(9) Method for matching procedures between CFG representations of the portions of programs;
(10) Computer readable medium storing CFG portion matching procedure program;
(11) Method for facilitating matching of blocks between CFG representations of the programs;
(12) Computer readable medium storing block matching facilitating program;
(13) Computer readable medium storing data structure comprising delta produced by delta generator system.

USE - For generating delta between program binaries.

ADVANTAGE - Common blocks of source and targets CFG's are matched in multiple passes so as to improve the matching by relaxing the criteria for a match and the register renaming problems is solved so that blocks can be fairly compared.

DESCRIPTION OF DRAWING(S) - The figure shows the schematic block

diagram of the minimum delta generator for program binaries.
Source program (112)
Target program (122)
Delta (142)
pp; 29 DwgNo 1/9

Title Terms: DELTA; GENERATE; METHOD; PROGRAM; BINARY; IDENTIFY; UNMATCHED; BLOCK; MERGE; SOURCE; CONTROL; FLOW; GRAPH; REPRESENT; SO; SOURCE; TARGET ; CONTROL; FLOW; GRAPH; IDENTICAL

Derwent Class: T01

International Patent Class (Main): **G06F-009/44** ; **G06F-011/00**

File Segment: EPI

6/5/16 (Item 16 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014615009 **Image available**
WPI Acc No: 2002-435713/200246
Related WPI Acc No: 2004-088364; 2004-213318
XRPX Acc No: N02-342963

Image hashing by deriving independent hash values for visually distinct images and identical values for similar images

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: KOON S W; **VENKATESAN R**
Number of Countries: 094 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200237331	A1	20020510	WO 2000US41359	A	20001019	200246	B
AU 200245857	A	20020515	WO 2000US41359	A	20001019	200258	
			AU 200245857	A	20001019		
EP 1327201	A1	20030716	EP 2000993908	A	20001019	200347	
			WO 2000US41359	A	20001019		
AU 2002245857	A8	20050915	AU 2002245857	A	20001019	200569	

Priority Applications (No Type Date): WO 2000US41359 A 20001019; US 99421986 A 19991019
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200237331	A1	E	30	G06F-017/30	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200245857	A			G06F-017/30	Based on patent WO 200237331
EP 1327201	A1	E		G06F-017/30	Based on patent WO 200237331
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
AU 2002245857	A8			G06F-017/30	Based on patent WO 200237331

Abstract (Basic): WO 200237331 A1

NOVELTY - Method consists in deriving a hash value representing the received image so that visually distinct images result in hash values that are approximately independent of each other and visually similar images result in identical hash values. The hash value is stored with the image to index it and watermark the image. Hash values from different images are compared.

DETAILED DESCRIPTION - There are INDEPENDENT CLAIMS for (1) a digital image processing system, (2) a digital image hash system, (3) a hash value program.

USE - Method is for hashing digital images in databases and can be used for on-line searches of web sites for detection of pirated copies..

ADVANTAGE - Method allows modest changes to an image which may or may not be perceptible to the eye without resulting in different hash values for the original and modified images.

DESCRIPTION OF DRAWING(S) - The figure shows a block diagram of an image distribution system.

pp; 30 DwgNo 1/6

Title Terms: IMAGE; HASH; DERIVATIVE; INDEPENDENT; HASH; VALUE; VISUAL; DISTINCT; IMAGE; IDENTICAL; VALUE; SIMILAR; IMAGE
Derwent Class: T01
International Patent Class (Main): **G06F-017/30**
International Patent Class (Additional): G06T-001/00
File Segment: EPI

6/5/17 (Item 17 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014419011 **Image available**
WPI Acc No: 2002-239714/200229
XRPX Acc No: N02-184885

Digital data distribution e.g. for software products, involves modifying initial digital goods such that modified digital goods is operatively different in configuration but functionally equivalent to initial digital goods

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **JAKUBOWSKI M H** ; PEINADO M; **VENKATESAN R**

Number of Countries: 093 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200169354	A2	20010920	WO 2001US1609	A	20010117	200229	B
AU 200132841	A	20010924	AU 200132841	A	20010117	200229	

Priority Applications (No Type Date): US 2000525206 A 20000314
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200169354	A2	E	44	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200132841	A		G06F-001/00	Based on patent WO 200169354

Abstract (Basic): WO 200169354 A2

NOVELTY - Initial digital goods is provided to a computer. The initial digital goods is modified using unique key data to selectively individualize the initial digital goods such that the modified digital goods is operatively different in configuration but functionally equivalent to the initial digital goods.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Recording medium containing instructions for distributing break once run everywhere (BORE) resistant digital goods;

(b) Arrangement for use in host computer;

(c) System for distributing BORE resistant digital goods

USE - For distribution of break once run everywhere (BORE) resistant digital data such as software, music, video and books.

ADVANTAGE - The BORE resistant digital goods distribution is easy and cost effective for digital goods developer or content producer to implement, and are not overly burdensome on the consumer. The modified digital goods is substantially difficult to undermine on any significant scale, since each copy is uniquely configured for use by an authorized consumer/computer.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart of computer network.

pp; 44 DwgNo 1/9

Title Terms: DIGITAL; DATA; DISTRIBUTE; SOFTWARE; PRODUCT; MODIFIED; INITIAL; DIGITAL; GOODS; MODIFIED; DIGITAL; GOODS; OPERATE; CONFIGURATION ; FUNCTION; EQUIVALENT; INITIAL; DIGITAL; GOODS
Derwent Class: T01; W04
International Patent Class (Main): **G06F-001/00**
File Segment: EPI

6/5/18 (Item 18 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014405299 **Image available**
WPI Acc No: 2002-226002/200228
XRPX Acc No: N02-173393
Computer readable media for crypto system, stores program which enables padding received value and converting to element of Jacobion curve processed to product identifier
Patent Assignee: LAUTER K E (LAUT-I); MONTGOMERY P L (MONT-I); VENKATESAN R (VENK-I)
Inventor: LAUTER K E; MONTGOMERY P L; **VENKATESAN R**
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020018560	A1	20020214	US 2000213573	P	20000622	200228 B
			US 2001886147	A	20010620	

Priority Applications (No Type Date): US 2000213573 P 20000622; US 2001886147 A 20010620
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020018560	A1		18	H04L-009/00	Provisional application US 2000213573

Abstract (Basic): US 20020018560 A1

NOVELTY - A value associated with copies of a product is received and padded using a recognizable pattern. The padded value is converted to a number represented by a particular number of bits. The number is converted to an element of Jacobion curve and the element is raised to a particular power. The result is compressed and output as a product identifier.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Product identifier validation method;
(b) Data encryption method.
(c) Data decryption method.
(d) Data encryption system.
(e) Data decryption system.

USE - For generating product identifier in crypto systems, for validating data in software media e.g. CD-ROM, DVD storing copies of application program such as word processing program, spreadsheet program, etc.

ADVANTAGE - Reduces the incidence of unauthorized copying of software product. A variety of different curves is used, and in one implementation the curve is a hyperelliptic curve over a finite field. The product identifier is validated by reversing encryption process and extracting padded value.

DESCRIPTION OF DRAWING(S) - The figure shows an exemplary system using a product identifier to validate software.

pp; 18 DwgNo 2/7

Title Terms: COMPUTER; READ; MEDIUM; SYSTEM; STORAGE; PROGRAM; ENABLE; PAD; RECEIVE; VALUE; CONVERT; ELEMENT; CURVE; PROCESS; PRODUCT; IDENTIFY
Derwent Class: T01; T03; W01
International Patent Class (Main): H04L-009/00
International Patent Class (Additional): **G06F-017/60**
File Segment: EPI

6/5/19 (Item 19 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014319263
WPI Acc No: 2002-139965/200218
XRPX Acc No: N02-105460

Access method for secure data held on remote computer involves a callable interface to invoke different instructions depending on the repository to be used

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **JAKUBOWSKI M H** ; KRISHNASWAMY V; MANFERDELLI J L; MARR M D
Number of Countries: 095 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200201334	A2	20020103	WO 2001US40899	A	20010608	200218	B
AU 200167056	A	20020108	AU 200167056	A	20010608	200235	
AU 2001267056	A8	20051013	AU 2001267056	A	20010608	200611	

Priority Applications (No Type Date): US 2000604518 A 20000627
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200201334	A2	E	65	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200167056	A	G06F-001/00	Based on patent WO 200201334
AU 2001267056	A8	G06F-001/00	Based on patent WO 200201334

Abstract (Basic): WO 200201334 A

NOVELTY - Decoupling interface is application programmer interface (API) usable with different dynamically linkable libraries. Each secure repository has hidden cryptographic key. Code that applies key without requiring access to copy of key. Code generated based on data identifying hardware resources available at computer being used. Code may also be based on a random number.

DETAILED DESCRIPTION - Decoupling interface provides a common communication and authentication interface for different secure repositories and acts to invoke the appropriate instructions for use by the selected repository. Functions implemented by repository include decryption and validation of cryptographically signed information.

INDEPENDENT CLAIMS are included for

(a) a method of communicating between a software process and one of a number of secure repositories

(b) a secure repository

(c) a method of communicating with one of a number of secure repositories

(d) a computer readable medium carrying instructions for communicating with one of a number of secure repositories

(e) and a method of authenticating a first software process to a second software process

USE - In software-based repositories.

ADVANTAGE - Allows the use of multiple secure repositories.

Dwg.0/9

Title Terms: ACCESS; METHOD; SECURE; DATA; HELD; REMOTE; COMPUTER; INTERFACE; INVOKE; INSTRUCTION; DEPEND; REPOSITORY
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/00**
File Segment: EPI

6/5/20 (Item 20 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014319262
WPI Acc No: 2002-139964/200218
XRPX Acc No: N02-105459

Cryptographic key method for providing a software-based secure repository by receiving data identifying the computer hardware and creating instructions for encrypting data on that hardware

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **JAKUBOWSKI M H** ; KRISHNASWAMY V; MANFERDELLI J L; MARR M D

Number of Countries: 095 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200201333	A2	20020103	WO 2001US40898	A	20010608	200218	B
AU 200167055	A	20020108	AU 200167055	A	20010608	200235	
AU 2001267055	A8	20051020	AU 2001267055	A	20010608	200615	

Priority Applications (No Type Date): US 2000604543 A 20000627
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200201333	A2	E	68	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200167055	A	G06F-001/00	Based on patent WO 200201333
AU 2001267055	A8	G06F-001/00	Based on patent WO 200201333

Abstract (Basic): WO 200201333 A

NOVELTY - Repository may be coupled to application program which uses secure services of repository by way of a decoupling interface which provides a common communication and authentication interface for different secure repositories and invokes the appropriate instructions for use by the selected repository. Decoupling interface may take form of single application programmer interface (API) usable with different dynamically linkable libraries.

DETAILED DESCRIPTION - The secure repository has a hidden cryptographic key and code that applies the key without requiring access to a copy of the key. The code is generated based in part upon data identifying the hardware resources available at the computer being used. The code may also be based on a random number. The functions implemented by the repository include decryption and validation of cryptographically signed information.

INDEPENDENT CLAIMS are included for

(a) a computer readable medium carrying instructions for using a cryptographic key

(b) a system for providing a secure repository

(c) a method of enabling the performance of an action on a computing device

(d) a system for performing an action on a computing device

(e) a method of using encrypted information at a computing device

(f) and a computer readable medium carrying instructions for using encrypted information at a computing device

USE - Providing a secure repository for data.

ADVANTAGE - provides a secure repository individualized for any suitable hardware.

Dwg.0/9

Title Terms: CRYPTOGRAPHIC; KEY; METHOD; SOFTWARE; BASED; SECURE; REPOSITORY; RECEIVE; DATA; IDENTIFY; COMPUTER; HARDWARE; INSTRUCTION; DATA; HARDWARE
Derwent Class: T01; W01

International Patent Class (Main): **G06F-001/00**
File Segment: EPI

6/5/21 (Item 21 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014319258 **Image available**
WPI Acc No: 2002-139960/200218
XRPX Acc No: N02-105455

Secure repository with layers of tamper resistance for providing computer security using hidden cryptographic key and code to apply key without requiring access to copy of key

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **JAKUBOWSKI M H** ; KRISHNASWAMY V; MANFERDELLI J L; MARR M D
Number of Countries: 095 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200201327	A2	20020103	WO 2001US18670	A	20010608	200218	B
AU 200166809	A	20020108	AU 200166809	A	20010608	200235	
AU 2001266809	A8	20051020	AU 2001266809	A	20010608	200615	

Priority Applications (No Type Date): US 2000604174 A 20000627
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200201327	A2	E	69	G06F-001/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW

AU 200166809	A	G06F-001/00	Based on patent WO 200201327
AU 2001266809	A8	G06F-001/00	Based on patent WO 200201327

Abstract (Basic): WO 200201327 A

NOVELTY - A cryptographic code generator (412) generates a code for inclusion in a block box (240), applying the cryptographic keys (248) and object keys from a database (408) and creating code to hide them in the black box. The key includes asymmetric or public/private key pairs, which are hidden in the sense that they are never actually represented in numerical form. The generator can also create code to use the key to validate cryptographic signals without requiring access to the key.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for a method of creating a computer program that uses a cryptographic algorithm and for a computer readable medium with instructions for securely decrypting data.

USE - Providing secure repository with layers of tamper resistance.

ADVANTAGE - Resisting discovery of secret keys.

DESCRIPTION OF DRAWING(S) - The drawing shows the repository
Code generator 412
Black box 240
Cryptographic key 248
Database 408
Dwg.4/9

Title Terms: SECURE; REPOSITORY; LAYER; TAMPER; RESISTANCE; COMPUTER; SECURE; HIDE; CRYPTOGRAPHIC; KEY; CODE; APPLY; KEY; REQUIRE; ACCESS; COPY ; KEY
Derwent Class: T01
International Patent Class (Main): **G06F-001/00**
File Segment: EPI

6/5/22 (Item 22 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014132082 **Image available**
WPI Acc No: 2001-616293/200171
XRPX Acc No: N01-459712

Cryptographic identifier forming apparatus for optical disk, has processor which integrally splices flow patterns of watermark and **non-marked codes based on selected execution flow and associated routine**

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: VAZIRANI V; **VENKATESAN R**

Number of Countries: 094 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200169355	A1	20010920	WO 2001US3821	A	20010207	200171 B
AU 200134861	A	20010924	AU 200134861	A	20010207	200208
US 6829710	B1	20041207	US 2000525694	A	20000314	200480
US 20040255132	A1	20041216	US 2000525694	A	20000314	200482
			US 2004880213	A	20040629	
US 20050144458	A1	20050630	US 2000525694	A	20000314	200543
			US 2004880213	A	20040629	
			US 2004970425	A	20041021	

Priority Applications (No Type Date): US 2000525694 A 20000314; US 2004880213 A 20040629; US 2004970425 A 20041021
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200169355	A1	E	68	G06F-001/00	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
AU 200134861	A			G06F-001/00	Based on patent WO 200169355
US 6829710	B1			H04L-009/00	
US 20040255132	A1			H04L-009/32	Cont of application US 2000525694
US 20050144458	A1			G06F-009/44	Cont of application US 2000525694
					Cont of application US 2004880213
					Cont of patent US 6829710

Abstract (Basic): WO 200169355 A1

NOVELTY - A processor randomly selects a nodal pair from input flow pattern. The processor establishes execution flow and the associated routine to splice the flow patterns of a watermark and an unmarked code integrally including all the different routing and associated execution flow.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Cryptographic identifier formation method;

(b) Computer readable medium containing instructions to form cryptographic identifier;

(c) Executable computer code marked with identifier

USE - For embedding highly tamper-resistant watermark codes to read only optical disks such as compact disk read only memory (CD-ROM), digital video disk (DVD), and magnetic disk which contains copyright of application software.

ADVANTAGE - Since the flow pattern is tightly spliced, removal of the watermark is effectively impossible. The codes for routines are added such that the flow pattern of watermarked code and an unmarked code are same, making the watermark highly tamper-proof.

DESCRIPTION OF DRAWING(S) - The figure shows a simplified high level block diagram of watermarking technique software.

pp; 68 DwgNo 3/10

Title Terms: CRYPTOGRAPHIC; IDENTIFY; FORMING; APPARATUS; OPTICAL; DISC; PROCESSOR; INTEGRAL; SPLICE; FLOW; PATTERN; WATERMARK; NON; MARK; CODE; BASED; SELECT; EXECUTE; FLOW; ASSOCIATE; ROUTINE
Derwent Class: T01
International Patent Class (Main): **G06F-001/00** ; **G06F-009/44** ; H04L-009/00; H04L-009/32
File Segment: EPI

6/5/23 (Item 23 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014112185 **Image available**
WPI Acc No: 2001-596397/200167
Related WPI Acc No: 2000-611744; 2000-647267; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2002-279866; 2002-350656; 2002-392575; 2003-522656; 2005-617252; 2005-701313
XRPX Acc No: N01-444633

Black box key file generating apparatus for digital rights management system, has code optimizer and key manager which produces key file which is forwarded to requesting management system

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: DAVIS M; PEINADO M; **VENKATESAN R**
Number of Countries: 092 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200152471	A1	20010719	WO 2000US23106	A	20000822	200167 B
AU 200069279	A	20010724	AU 200069279	A	20000822	200168

Priority Applications (No Type Date): US 2000525509 A 20000315; US 2000176425 P 20000114
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200152471	A1	E	130	H04L-009/08	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW

AU 200069279	A		H04L-009/08	Based on patent WO 200152471

Abstract (Basic): WO 200152471 A1

NOVELTY - A code optimizer receives a master executable and randomized optimization parameters as inputs and produces corresponding outputs. A key manager (84) receives an initial key file (82) and set of current black box keys as input, to produce a key file including set of keys of current and initial black boxes. The key file (81) is forwarded to requesting digital rights management system.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for method for generating new black box key file.

USE - Use in digital rights management systems for enforcing rights on digital contents like digital audios, digital videos, digital data, digital text, digital multimedias, etc.

ADVANTAGE - A flexible and content owner controllable digital enforcement for digital content is achieved by forwarding the nth executable and the nth key file which is extracted by key manager to the requesting DRM system.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of black box key file generating apparatus.

Key file (81)
Initial key file (82)
Key manager (84)
pp; 130 DwgNo 19/22

Title Terms: BLACK; BOX; KEY; FILE; GENERATE; APPARATUS; DIGITAL; MANAGEMENT; SYSTEM; CODE; OPTIMUM; KEY; MANAGE; PRODUCE; KEY; FILE; FORWARDING; REQUEST; MANAGEMENT; SYSTEM
Derwent Class: T01; W01
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): **G06F-001/00**
File Segment: EPI

6/5/24 (Item 24 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014112116 **Image available**
WPI Acc No: 2001-596328/200167
Related WPI Acc No: 2000-611744; 2000-647267; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596397; 2002-279866; 2002-350656; 2002-392575; 2003-522656; 2005-617252; 2005-701313
XRPX Acc No: N01-444564

Encrypting a digital object based on key ID selected for the digital object, using selected key ID as input to a selected function output of which is used as key for the digital object

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: PEINADO M; **VENKATESAN R**
Number of Countries: 092 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200152019	A1	20010719	WO 2000US23105	A	20000822	200167 B
AU 200069278	A	20010724	AU 200069278	A	20000822	200168
US 6816596	B1	20041109	US 2000176425	P	20000114	200474
			US 2000526292	A	20000315	
US 20050066187	A1	20050324	US 99126614	P	19990327	200526
			US 2000176425	P	20000114	
			US 2000526292	A	20000315	
			US 2004981846	A	20041105	
US 20050086478	A1	20050421	US 99126614	P	19990327	200528
			US 2000176425	P	20000114	
			US 2000526292	A	20000315	
			US 2004982105	A	20041105	
US 7016498	B2	20060321	US 99126614	P	19990327	200621
			US 2000176425	P	20000114	
			US 2000526292	A	20000315	
			US 2004982105	A	20041105	

Priority Applications (No Type Date): US 2000526292 A 20000315; US 2000176425 P 20000114; US 99126614 P 19990327; US 2004981846 A 20041105; US 2004982105 A 20041105
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200152019	A1	E	130	G06F-001/00	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200069278	A			G06F-001/00	Based on patent WO 200152019
US 6816596	B1			H04L-009/00	Provisional application US 2000176425
US 20050066187	A1			H04L-009/00	Provisional application US 99126614 Provisional application US 2000176425 Cont of application US 2000526292 Cont of patent US 6816596
US 20050086478	A1			H04L-009/00	Provisional application US 99126614 Provisional application US 2000176425 Cont of application US 2000526292 Cont of patent US 6816596
US 7016498	B2			H04L-009/00	Provisional application US 99126614 Provisional application US 2000176425 Cont of application US 2000526292 Cont of patent US 6816596

Abstract (Basic): WO 200152019 A1

NOVELTY - The digital object is encrypted according to the key and distributed along with the key ID. The key ID is selected according to a member selected from a group randomly and serially, and used along with a secret seed as input to the function. The output of the function is used as a symmetric encryption and decryption key for the digital object.

DETAILED DESCRIPTION - AN INDEPENDENT CLAIM is made for:

(a) A method of producing a key for decrypting an encrypted digital object;

(b) A method of requesting a key for decrypting an encrypted digital object;

(c) A method of producing a security key.

USE - For enforcing rights in digital content, such that enforcement architecture allows access to encrypted digital content only in accordance with parameters specified by license rights acquired by user of the digital content, such as digital audio, digital video, digital text, digital data, and digital multimedia for distribution to users.

ADVANTAGE - Invention allows owner of digital content to specify license rules that must be satisfied before such digital content is allowed to be rendered e.g. on user's computing device.

DESCRIPTION OF DRAWING(S) - Figure shows a flow diagram of various steps performed during derivation of a decryption key from a key ID.

pp; 130 DwgNo 18/22

Title Terms: DIGITAL; OBJECT; BASED; KEY; ID; SELECT; DIGITAL; OBJECT; SELECT; KEY; ID; INPUT; SELECT; FUNCTION; OUTPUT; KEY; DIGITAL; OBJECT

Derwent Class: T01; W01; W02; W04

International Patent Class (Main): **G06F-001/00** ; H04L-009/00

International Patent Class (Additional): **G06F-012/14** ; H04L-009/08; H04L-009/28; H04L-009/30

File Segment: EPI

6/5/25 (Item 25 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013858777 **Image available**
WPI Acc No: 2001-342990/200136
XRPX Acc No: N01-248413

Cryptographic process for use in personal computer, involves implementing primitive of preset sequence of order manipulations, by addition and multiplication operations

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: **JAKUBOWSKI M** ; **VENKATESAN R**
Number of Countries: 092 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200078118	A2	20001228	WO 2000US16035	A	20000609	200136	B
AU 200079816	A	20010109	AU 200079816	A	20000606	200136	
US 6570988	B1	20030527	US 99329139	A	19990609	200337	
JP 2003526118	W	20030902	WO 2000US16035	A	20000609	200358	
			JP 2001504202	A	20000609		
EP 1468521	A2	20041020	EP 2000970432	A	20000609	200469	
			WO 2000US16035	A	20000609		
EP 1468521	B1	20060322	EP 2000970432	A	20000609	200622	
			WO 2000US16035	A	20000609		

Priority Applications (No Type Date): US 99329139 A 19990609
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200078118	A2	E	42	G06F-007/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200079816	A			G06F-007/00	Based on patent WO 200078118
US 6570988	B1			H04L-009/28	
JP 2003526118	W		33	G09C-001/00	Based on patent WO 200078118
EP 1468521	A2	E		H04L-009/32	Based on patent WO 200078118
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
EP 1468521	B1	E		H04L-009/32	Based on patent WO 200078118
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					

Abstract (Basic): WO 200078118 A2

NOVELTY - The input digital plain text or cipher text block is converted into the output digital cipher text or plain text block by predefined sequence of order manipulations as the primitive, additions and mod (2n) multiplication operations where n' is a predefined integer. The addition and multiplication collectively implement the primitive, but without calculating a value for mod (Mn).

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Computer readable medium;

(b) Apparatus for encrypting or decrypting block of input digital plain text or cipher text

USE - For use in highly sophisticated general purpose devices e.g. personal computers and workstations and simple dedicated devices e.g. smart cards, remote controls and electronic appliances for encrypting or decrypting block of input digital plain text or cipher text.

ADVANTAGE - The primitive is implemented for computing a checksum without any need for modem operation, hence processing time is reduced.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram explaining the cryptographic process.

pp; 42 DwgNo 1/6
Title Terms: CRYPTOGRAPHIC; PROCESS; PERSON; COMPUTER; IMPLEMENT; PRIMITIVE ; PRESET; SEQUENCE; ORDER; MANIPULATE; ADD; MULTIPLICATION; OPERATE
Derwent Class: P85; T01; W01
International Patent Class (Main): **G06F-007/00** ; G09C-001/00; H04L-009/28; H04L-009/32
File Segment: EPI; EngPI

6/5/26 (Item 26 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013851053 **Image available**
WPI Acc No: 2001-335266/200135
XRPX Acc No: N01-242009

Cryptographic parameter generation e.g. for message communication in Internet, involves performing multiplication, order manipulation and addition to replace complex modular operation, when processing message block

Patent Assignee: MICROSOFT CORP (MICT); JAKUBOWSKI M (JAKU-I); VENKATESAN R (VENK-I)
Inventor: **JAKUBOWSKI M H** ; **VENKATESAN R** ; **JAKUBOWSKI M**
Number of Countries: 092 Number of Patents: 011
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200075750	A2	20001214	WO 2000US15871	A	20000609	200135	B
AU 200074695	A	20001228	AU 200074695	A	20000609	200135	
EP 1208416	A2	20020529	EP 2000963254	A	20000609	200243	
			WO 2000US15871	A	20000609		
US 20020110239	A1	20020815	US 99329138	A	19990609	200256	
US 6483918	B2	20021119	US 99329138	A	19990609	200280	
JP 2003501698	W	20030114	WO 2000US15871	A	20000609	200306	
			JP 2001501960	A	20000609		
EP 1208416	B1	20050413	EP 2000963254	A	20000609	200525	
			WO 2000US15871	A	20000609		
DE 60019432	E	20050519	DE 19432	A	20000609	200535	
			EP 2000963254	A	20000609		
			WO 2000US15871	A	20000609		
EP 1555777	A2	20050720	EP 2000963254	A	20000609	200547	
			EP 20057754	A	20000609		
ES 2235946	T3	20050716	EP 2000963254	A	20000609	200549	
DE 60019432	T2	20050901	DE 19432	A	20000609	200559	
			EP 2000963254	A	20000609		
			WO 2000US15871	A	20000609		

Priority Applications (No Type Date): US 99329138 A 19990609
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200075750	A2	E	46	G06F-000/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200074695	A			G06F-000/00	Based on patent WO 200075750
EP 1208416	A2	E		G06F-001/00	Based on patent WO 200075750
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
US 20020110239	A1			H04L-009/18	
US 6483918	B2			H04L-009/28	
JP 2003501698	W		38	G09C-001/00	Based on patent WO 200075750
EP 1208416	B1	E		G06F-001/00	Based on patent WO 200075750
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
DE 60019432	E			G06F-001/00	Based on patent EP 1208416 Based on patent WO 200075750
EP 1555777	A2	E		H04L-009/32	Div ex application EP 2000963254 Div ex patent EP 1208416
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
ES 2235946	T3			G06F-001/00	Based on patent EP 1208416

DE 60019432 T2 G06F-001/00 Based on patent EP 1208416
Based on patent WO 200075750

Abstract (Basic): WO 200075750 A2

NOVELTY - Blocks of plain text input image are processed through a primitive that uses a predefined function f(x)=ax+bmod(M) for generating the parameter, where a,b are integers and M is integer prime number. The primitive replaces mod(M) operation by mod 2n multiplication, order manipulation like byte or word swap and addition operation.

DETAILED DESCRIPTION - A processor computes predefined intermediate processing results y=F(x) of message blocks through the primitive. The intermediate results are concatenated to produce the parameter. INDEPENDENT CLAIMS are also included for the following:

(a) Computer readable medium;

(b) parameter generating apparatus

USE - For generating cryptographic parameter e.g. checksum (MAC) are stream cipher without modular operation for encryption/decryption of message and to protect information in PC, workstation, smart cards, remote controls and electronic appliances. Also for providing secured electronic communication in computer network e.g. E-mail communication in Internet.

ADVANTAGE - Replaces complex modular operation by simple elementary register operations hence reduces processing time and cost to a greater extent.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram explaining cryptographic process used to generate MAC.

pp; 46 DwgNo 1/6

Title Terms: CRYPTOGRAPHIC; PARAMETER; GENERATE; MESSAGE; COMMUNICATE; PERFORMANCE; MULTIPLICATION; ORDER; MANIPULATE; ADD; REPLACE; COMPLEX; MODULE; OPERATE; PROCESS; MESSAGE; BLOCK

Derwent Class: P85; T01; W01

International Patent Class (Main): **G06F-000/00** ; **G06F-001/00** ; G09C-001/00; H04L-009/18; H04L-009/28; H04L-009/32

International Patent Class (Additional): H04L-009/32

File Segment: EPI; EngPI

6/5/27 (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013706946 **Image available**
WPI Acc No: 2001-191170/200119
Related WPI Acc No: 2000-611744; 2000-647267; 2000-647268; 2001-090815; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2001-596397; 2002-279866; 2002-350656; 2002-392575; 2003-522656; 2005-617252; 2005-701313
XRPX Acc No: N01-135885

Black box obtaining method of digital rights management system in personal computer, by determining unique black box having public and private key pair to digital rights management system from black box server

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: ENGLAND P; PEINADO M; **VENKATESAN R**
Number of Countries: 089 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200057684	A2	20001005	WO 2000US4946	A	20000225	200119	B
AU 200033809	A	20001016	AU 200033809	A	20000225	200119	

Priority Applications (No Type Date): US 2000482840 A 20000113; US 99126614 P 19990327; US 99290363 A 19990412
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200057684	A2	E	87	G06F-007/00	

Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW

AU 200033809	A		Based on patent WO 200057684

Abstract (Basic): WO 200057684 A2

NOVELTY - A unique black box having a public and private key pair is generated by a black box server, in response to a request from digital rights management system (DRM). The black box is then delivered to the DRM which then installs the black box.

DETAILED DESCRIPTION - The DRM requests for black box to the black box server via Internet connection when the previously installed black box is not current or non-unique. The black box is generated by the black server and delivered to the DRAM along with an identifying indicating currency, version number, digital certificate. A portion of the private key of the generated black box is encrypted according to software code associated with generated black box. An INDEPENDENT CLAIM is also included for black box obtaining program.

USE - For enforcing rights in digital content such as digital audio, digital text, digital multimedia in personal computer.

ADVANTAGE - Prevents user of the computing device from making copy of digital content, except allowed by the content owner.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram illustrating the steps performed in connection with DRM system.

pp; 87 DwgNo 9/12

Title Terms: BLACK; BOX; OBTAIN; METHOD; DIGITAL; MANAGEMENT; SYSTEM; PERSON; COMPUTER; DETERMINE; UNIQUE; BLACK; BOX; PUBLIC; PRIVATE; KEY; PAIR; DIGITAL; MANAGEMENT; SYSTEM; BLACK; BOX; SERVE
Derwent Class: T01; T03; W04
International Patent Class (Main): **G06F-007/00**
File Segment: EPI

6/5/28 (Item 28 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013475324 **Image available**
WPI Acc No: 2000-647267/200062
Related WPI Acc No: 2000-611744; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2001-596397; 2002-279866; 2002-350656; 2002-392575; 2003-522656; 2005-617252; 2005-701313
XRPX Acc No: N00-479688

Enforcement architecture for digital rights management, determines whether right to render digital content in manner sought exists based on digital license stored in computing device

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: ABBURI R; BELL J R C; BLINN A N; ENGLAND P; **JAKUBOWSKI M H** ; JONES T C; MANFERDELLI J L; PEINADO M; **VENKATESAN R** ; YU H Y V
Number of Countries: 090 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200059150	A2	20001005	WO 2000US4947	A	20000225	200062	B
AU 200035039	A	20001016	AU 200035039	A	20000225	200106	
EP 1287636	A2	20030305	EP 2000913629	A	20000225	200319	
			WO 2000US4947	A	20000225		
JP 2003536119	W	20031202	JP 2000608539	A	20000225	200382	
			WO 2000US4947	A	20000225		

Priority Applications (No Type Date): US 99290363 A 19990412; US 99126614 P 19990327
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200059150	A2	E	90	H04L-009/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW					
AU 200035039	A			H04L-009/00	Based on patent WO 200059150
EP 1287636	A2	E		H04L-009/00	Based on patent WO 200059150
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
JP 2003536119	W		101	G06F-017/60	Based on patent WO 200059150

Abstract (Basic): WO 200059150 A2

NOVELTY - A computing device (14) receives distributed digital content from a content server (22) and stores digital license corresponding to the digital content (12). A digital rights management (DRM) system on the computing device is invoked by a rendering application and determines whether a right to render digital content in the manner sought exists based on digital license stored in the computing device.

DETAILED DESCRIPTION - The digital content (12) in encrypted form is distributed by content server and a license server (24) issues digital license corresponding to the digital content. The content and license servers are communicatively coupled to internet. The digital license includes a decryption key for decrypting the encrypted digital content and a description of rights conferred by the license. An INDEPENDENT CLAIM is also included for digital rights management implementing method.

USE - For allowing access to digital contents such as digital audio, video, text and digital multimedia and enforcing rights in protected digital content on a medium such as internet, optical disk. For handheld devices, multiprocessor systems, microprocessor based or

programmable consumer electronics, network PCs, mini computers, main frame computers.

ADVANTAGE - Prevents user of the computing device from making a copy of digital content, except otherwise allowed by content owner. Enables user to obtain license from a license server without any action necessary on the part of the user.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of enforcement architecture.

Digital content (12)

Computing device (14)

Servers (22,24)

pp; 90 DwgNo 1/12

Title Terms: ARCHITECTURE; DIGITAL; MANAGEMENT; DETERMINE; RIGHT; RENDER; DIGITAL; CONTENT; MANNER; EXIST; BASED; DIGITAL; LICENCE; STORAGE; COMPUTATION; DEVICE

Derwent Class: W01

International Patent Class (Main): **G06F-017/60** ; H04L-009/00

International Patent Class (Additional): **G06F-015/00** ; H04L-009/08; H04L-009/32

File Segment: EPI

6/5/29 (Item 29 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013439801 **Image available**
WPI Acc No: 2000-611744/200058
Related WPI Acc No: 2000-647267; 2000-647268; 2001-090815; 2001-191170; 2001-210824; 2001-210825; 2001-496746; 2001-522158; 2001-522159; 2001-596328; 2001-596397; 2002-279866; 2002-392575; 2003-522656; 2005-617252; 2005-701313
XRPX Acc No: N00-452991

Interdependent validation for digital rights management and enforcement, involves deriving key from device source for applying to digital signature from digital content package to validate digital content package

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: PEINADO M; **VENKATESAN R** ; ABBURI R; BELL J R C; BLINN A N; JONES T C
Number of Countries: 090 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 200059152	A2	20001005	WO 2000US4983	A	20000225	200058 B
AU 200036081	A	20001016	AU 200036081	A	20000225	200106
US 20050086478	A1	20050421	US 99126614	P	19990327	200528
			US 2000176425	P	20000114	
			US 2000526292	A	20000315	
			US 2004982105	A	20041105	
US 20050091169	A1	20050428	US 99126614	P	19990327	200530
			US 2000176425	P	20000114	
			US 2000526291	A	20000315	
			US 2004982578	A	20041105	
US 20050091541	A1	20050428	US 99126614	P	19990327	200530
			US 2000176425	P	20000114	
			US 2000526291	A	20000315	
			US 2004980743	A	20041103	
US 6973444	B1	20051206	US 99126614	P	19990327	200580
			US 99290363	A	19990412	
			US 2000482928	A	20000113	

Priority Applications (No Type Date): US 2000482928 A 20000113; US 99126614 P 19990327; US 99290363 A 19990412; US 2000176425 P 20000114; US 2000526292 A 20000315; US 2004982105 A 20041105; US 2000526291 A 20000315 ; US 2004982578 A 20041105; US 2004980743 A 20041103
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200059152	A2	E	85	H04L-009/00	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW				
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ TZ UG ZW					
AU 200036081	A			H04L-009/00	Based on patent WO 200059152
US 20050086478	A1			H04L-009/00	Provisional application US 99126614
					Provisional application US 2000176425
					Cont of application US 2000526292
					Cont of patent US 6816596
US 20050091169	A1			H04L-009/00	Provisional application US 99126614
					Provisional application US 2000176425
					Cont of application US 2000526291
					Cont of patent US 6829708
US 20050091541	A1			G06F-011/30	Provisional application US 99126614

			Provisional application US 2000176425 Cont of application US 2000526291
US 6973444	B1	G06F-017/00	Provisional application US 99126614 Cont of application US 99290363

Abstract (Basic): WO 200059152 A2

NOVELTY - The method involves deriving a key from a source available to a device. A digital signature is obtained from a digital content package for applying the key to digital signature to validate the digital signature and digital content package. The key used on the digital signature is derived for applying the key to a digital signature from the license to validate the digital signature and the license.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for computer readable medium.

USE - Used in digital rights management and enforcement of digital content like digital audio, digital video, digital text, digital data, digital multimedia, etc.

ADVANTAGE - The user of a computing device is prevented from making a copy of the digital contents except allowed by the content owner is achieved by deriving a key from the device source which is applied to the digital signature obtained from the digital content package for validating the digital content package.

DESCRIPTION OF DRAWING(S) - The figure shows the flow diagram showing the key transaction steps to validate a license and a piece of digital content.

pp; 85 DwgNo 10/12

Title Terms: INTERDEPENDENT; VALID; DIGITAL; MANAGEMENT; DERIVATIVE; KEY; DEVICE; SOURCE; APPLY; DIGITAL; SIGNATURE; DIGITAL; CONTENT; PACKAGE; VALID; DIGITAL; CONTENT; PACKAGE

Derwent Class: T01; W01; W02; W04

International Patent Class (Main): **G06F-011/30** ; **G06F-017/00** ; H04L-009/00

International Patent Class (Additional): **G06F-017/60**

File Segment: EPI

6/5/30 (Item 30 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012934585 **Image available**
WPI Acc No: 2000-106432/200009
XRPX Acc No: N00-081747

Method for generating, for given message to be signed, authentic cryptographic signature that can be authenticated by recipient of signed message as having come from signer of message

Patent Assignee: MICROSOFT CORP (MICT)
Inventor: MONTGOMERY P L; **VENKATESAN R R**
Number of Countries: 087 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9967920	A1	19991229	WO 99US14215	A	19990623	200009	B
AU 9954576	A	20000110	AU 9954576	A	19990623	200025	
US 6163841	A	20001219	US 98102851	A	19980623	200102	
US 6209093	B1	20010327	US 98102948	A	19980623	200119	
EP 1088420	A1	20010404	EP 99940794	A	19990623	200120	
			WO 99US14215	A	19990623		
CN 1306714	A	20010801	CN 99807748	A	19990623	200172	
JP 2002519723	W	20020702	WO 99US14215	A	19990623	200246	
			JP 2000556476	A	19990623		
CN 1534922	A	20041006	CN 99807748	A	19990623	200506	
			CN 200432591	A	19990623		

Priority Applications (No Type Date): US 98102948 A 19980623; US 98102851 A 19980623
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9967920	A1	E	60	H04L-009/32	
Designated States (National): AE AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SL SZ UG ZW					
AU 9954576	A			H04L-009/32	Based on patent WO 9967920
US 6163841	A			H04L-009/00	
US 6209093	B1			H04L-009/00	
EP 1088420	A1	E		H04L-009/32	Based on patent WO 9967920
Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE					
CN 1306714	A			H04L-009/32	
JP 2002519723	W		84	G09C-001/00	Based on patent WO 9967920
CN 1534922	A			H04L-009/32	Div ex application CN 99807748

Abstract (Basic): WO 9967920 A1

NOVELTY - Authentic signature is generated using generator value in conjunction with 3 keys, public, private and secret keys, which increases security associated with cryptographic signatures generated via conventional 2-key public key system. A unique product copy indicia (75) is formed by concatenating an identifier, for a given copy (70), with its corresponding authentic signature, used later by the user.

USE - For producing privately authenticatable cryptographic signatures and for using these signatures in conjunction with a product copy.

ADVANTAGE - Knowledge of the public and private keys alone is quite insufficient to permit persons, without knowledge of the secret key, to generate a new signed message pair containing an authentic signature.

DESCRIPTION OF DRAWING(S) - The drawing shows a high level simplified block diagram of CD-ROM production system 5 that incorporates the system.

the indicia for the unique product copy (75)

the product copy of the CD ROM package (70)
pp; 60 DwgNo 2/5
Title Terms: METHOD; GENERATE; MESSAGE; SIGN; AUTHENTICITY; CRYPTOGRAPHIC; SIGNATURE; CAN; AUTHENTICITY; RECIPIENT; SIGN; MESSAGE; MESSAGE
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00; H04L-009/00; H04L-009/32
International Patent Class (Additional): **G06F-001/00** ; G09F-001/00
File Segment: EPI; EngPI

6/5/31 (Item 31 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011742919 **Image available**
WPI Acc No: 1998-159829/199814
XRPX Acc No: N98-126986

Public key cryptography accelerating method - including security parameter database, control module, operating system and pre-computation device with precomputation off-line reducing amount of discrete exponentiation with long integers performed on-line

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)
Inventor: BOYKO V; **VENKATESAN R**
Number of Countries: 020 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9807253	A1	19980219	WO 97US14573	A	19970815	199814	B
EP 916208	A1	19990519	EP 97938422	A	19970815	199924	
			WO 97US14573	A	19970815		
JP 2000500886	W	20000125	WO 97US14573	A	19970815	200016	
			JP 98510103	A	19970815		
US 6091819	A	20000718	US 9623954	A	19960816	200037	
			US 97912251	A	19970815		
CA 2262549	C	20010612	CA 2262549	A	19970815	200136	
			WO 97US14573	A	19970815		

Priority Applications (No Type Date): US 9623954 P 19960816; US 97912251 A 19970815
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9807253	A1	E	29	H04L-009/30	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 916208	A1	E			Based on patent WO 9807253
Designated States (Regional): DE FI FR GB IT SE					
JP 2000500886	W		39	G09C-001/00	Based on patent WO 9807253
US 6091819	A			H04L-009/30	Provisional application US 9623954
CA 2262549	C	E		G06F-001/02	Based on patent WO 9807253

Abstract (Basic): WO 9807253 A

The method involves choosing integers k and n, with the number of ways of choosing k members from a set of n numbers is sufficiently large. Positive integers are randomly chosen and for each integer a value beta is computed. The integers and the beta are stored in pairs in a table. When a private key and public keys are desired, k pairs from the table are randomly selected.

The private key is evaluated as a sum of integers of the selected pairs and the sum is evaluated. The online steps are restarted if the sum is zero. The public key is evaluated as a product of the beta of the selected pairs and the product is evaluated.

ADVANTAGE - Increased speed in calculating second and subsequent key pairs.

Dwg.1/6

Title Terms: PUBLIC; KEY; ACCELERATE; METHOD; SECURE; PARAMETER; DATABASE; CONTROL; MODULE; OPERATE; SYSTEM; PRE; COMPUTATION; DEVICE; OFF-LINE; REDUCE; AMOUNT; DISCRETE; LONG; INTEGER; PERFORMANCE; ON-LINE
Derwent Class: P85; W01
International Patent Class (Main): **G06F-001/02** ; G09C-001/00; H04L-009/30
International Patent Class (Additional): **G06F-007/72** ; **G06F-017/10** ; H04L-009/00
File Segment: EPI; EngPI

6/5/32 (Item 32 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011742918 **Image available**
WPI Acc No: 1998-159828/199814
XRPX Acc No: N98-126985

Random number stretching method e.g. for secure pseudo random bit generator - having front end generator, selector, random function processor, graph processor and bit wise exclusive-or circuit with pseudo random bit generator stretching bit strings by use of certain one way functions which act on bit strings

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)
Inventor: AIELLO W A; RAJAGOPALAN S; **VENKATESAN R**
Number of Countries: 020 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9807251	A1	19980219	WO 97US14574	A	19970815	199814 B
EP 906678	A1	19990407	EP 97942381	A	19970815	199918
			WO 97US14574	A	19970815	
JP 2000502822	W	20000307	WO 97US14574	A	19970815	200023
			JP 98510104	A	19970815	
US 6104811	A	20000815	US 9623960	A	19960816	200041
			US 9735220	A	19970108	
			US 97911690	A	19970815	
CA 2262551	C	20020917	CA 2262551	A	19970815	200267
			WO 97US14574	A	19970815	

Priority Applications (No Type Date): US 9735220 P 19970108; US 9623960 P 19960816; US 97911690 A 19970815
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9807251	A1	E	19	H04L-009/00	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 906678	A1	E			Based on patent WO 9807251
Designated States (Regional): DE FI FR GB IT SE					
JP 2000502822	W		27	G09C-001/00	Based on patent WO 9807251
US 6104811	A			H04L-009/00	Provisional application US 9623960
					Provisional application US 9735220
CA 2262551	C	E		H04L-009/28	Based on patent WO 9807251

Abstract (Basic): WO 9807251 A

The method involves receiving a random number. A one-way function is performed on the random number to provide a longer random number. the longer random number is used as a one-time pad for encryption. The step of receiving the random number comprises receiving a cryptographically secure random number.

The step of performing the one-way function involves performing a cryptographic function which behaves like a random function. The step of performing the one-way function involves performing several one-way functions on the random number to generate several longer random numbers. The longer random numbers are concatenated.

ADVANTAGE - Increased speed and secure encryption.

Dwg.1/3

Title Terms: RANDOM; NUMBER; STRETCH; METHOD; SECURE; PSEUDO; RANDOM; BIT; GENERATOR; FRONT; END; GENERATOR; SELECT; RANDOM; FUNCTION; PROCESSOR; GRAPH; PROCESSOR; BIT; WISE; EXCLUSIVE-OR; CIRCUIT; PSEUDO; RANDOM; BIT; GENERATOR; STRETCH; BIT; STRING; ONE; WAY; FUNCTION; ACT; BIT; STRING
Derwent Class: P85; W01
International Patent Class (Main): G09C-001/00; H04L-009/00; H04L-009/28
International Patent Class (Additional): **G06F-001/02** ; **G06F-007/58** ;

H04L-009/22
File Segment: EPI; EngPI

6/5/33 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011332862 **Image available**
WPI Acc No: 1997-310766/199728
XRPX Acc No: N97-257397

Seed generator method for cryptographically strong bit streams - involves using first seed generator and random key generator to produce iterative outputs that are combined with two other seeds

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)
Inventor: AIELLO W A; **VENKATESAN R**
Number of Countries: 020 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9720266	A1	19970605	WO 96US17103	A	19961025	199728	B
US 5727063	A	19980310	US 95562925	A	19951127	199817	
EP 864124	A1	19980916	EP 96936951	A	19961025	199841	
			WO 96US17103	A	19961025		
JP 11500849	W	19990119	WO 96US17103	A	19961025	199913	
			JP 97520475	A	19961025		
JP 2963929	B2	19991018	WO 96US17103	A	19961025	199949	
			JP 97520475	A	19961025		
CA 2238545	C	20001212	CA 2238545	A	19961025	200103	
			WO 96US17103	A	19961025		

Priority Applications (No Type Date): US 95562925 A 19951127
Cited Patents: US 5297207; US 5327365; US 5412587; US 5420928; US 5515307
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9720266	A1	E	17	G06F-001/02	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
US 5727063	A		10	H04L-009/00	
EP 864124	A1	E		G06F-001/02	Based on patent WO 9720266
Designated States (Regional): DE FR GB IE IT					
JP 11500849	W		22	G06F-007/58	Based on patent WO 9720266
JP 2963929	B2		11	G06F-007/58	Previous Publ. patent JP 11500849 Based on patent WO 9720266
CA 2238545	C	E		G06F-007/58	Based on patent WO 9720266

Abstract (Basic): WO 9720266 A

The seed generator method involves using three seed generators. A first seed generator (510) is applied to an input register (530). A serial block cipher encoder (550) implements a function (F) based on the input register or a random key generator (540) for the first random key. The encoder's output is used as feedback to its input.

An inner product circuit (560) receives the input to the encoder and also inputs from second (520) and third (570) seed generators. It also has a random key input (542). The inner products are XOR'ed and parity bits used as the output (561).

ADVANTAGE - Provides output that is cryptographically strong and has no feasible procedure to separate it from truly random sequences.

Dwg.5/6

Title Terms: SEED; GENERATOR; METHOD; STRONG; BIT; STREAM; FIRST; SEED; GENERATOR; RANDOM; KEY; GENERATOR; PRODUCE; ITERATIVE; OUTPUT; COMBINATION; TWO; SEED
Derwent Class: P85; T01; W01
International Patent Class (Main): **G06F-001/02** ; **G06F-007/58** ; H04L-009/00
International Patent Class (Additional): G09C-001/00
File Segment: EPI; EngPI

6/5/34 (Item 34 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011186856 **Image available**
WPI Acc No: 1997-164781/199715
XRPX Acc No: N97-135786

Cryptographic hash function generation method for virus protection and data security - involves partitioning input bits into new set of blocks and processing new set of blocks with universal hash function generator arrangement to produce new set of keys

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)
Inventor: AIELLO W A; **VENKATESAN R**

Number of Countries: 020 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5608801	A	19970304	US 95559213	A	19951116	199715	B
WO 9718652	A1	19970522	WO 96US17449	A	19961031	199726	
EP 861539	A1	19980902	EP 96941950	A	19961031	199839	
			WO 96US17449	A	19961031		
JP 11500241	W	19990106	WO 96US17449	A	19961031	199911	
			JP 97518885	A	19961031		
CA 2237941	C	20010227	CA 2237941	A	19961031	200115	
			WO 96US17449	A	19961031		
JP 3187843	B2	20010716	WO 96US17449	A	19961031	200142	
			JP 97518885	A	19961031		

Priority Applications (No Type Date): US 95559213 A 19951116
Cited Patents: US 4928310
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5608801	A		14	H04L-009/00	
WO 9718652	A1	E	28	H04L-009/00	
Designated States (National): CA JP					
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE					
EP 861539	A1	E		H04L-009/00	Based on patent WO 9718652
Designated States (Regional): DE FR GB IE IT					
JP 11500241	W		34	G09C-001/00	Based on patent WO 9718652
CA 2237941	C	E		H04L-009/28	Based on patent WO 9718652
JP 3187843	B2		15	G09C-001/00	Previous Publ. patent JP 11500241 Based on patent WO 9718652

Abstract (Basic): US 5608801 A

The method involves partitioning input bits into a new set of blocks and processing new set of blocks with the universal hash function generator arrangement to produce a new set of keys. The new set of keys are inputted to the butterfly generator, to generate a set of bits. The exclusive-OR of the set of bits and the fed-back output of the butterfly generator are generated to produce a set of exclusively-ORed bits. The set of exclusively-ORed bits is processed by butterfly generator. The output of the butterfly generator has set of exclusively-ORed bits as input is the current hash function. The output of the butterfly generator upon the processing of all input bits is the cryptographic hash function.

ADVANTAGE - Uses strong pseudo-random generator. Uses input data to create high quality pseudo-random keys.

Dwg.5/6

Title Terms: CRYPTOGRAPHIC; HASH; FUNCTION; GENERATE; METHOD; VIRUS; PROTECT; DATA; SECURE; PARTITION; INPUT; BIT; NEW; SET; BLOCK; PROCESS; NEW; SET; BLOCK; UNIVERSAL; HASH; FUNCTION; GENERATOR; ARRANGE; PRODUCE; NEW; SET; KEY
Derwent Class: P85; T01; U23; W01

International Patent Class (Main): G09C-001/00; H04L-009/00; H04L-009/28
International Patent Class (Additional): **G06F-001/02** ; H03B-029/00;
H03M-007/00
File Segment: EPI; EngPI

6/5/35 (Item 35 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010742100 **Image available**
WPI Acc No: 1996-239055/199624
XRPX Acc No: N96-200127

Cryptographically strong pseudo-random bit generation - using unpredicatability properties of relatively slow cryptographically strong generator and rapid mixing properties of random walks on expander graphs

Patent Assignee: BELL COMMUNICATIONS RES (BELL-N)
Inventor: AIELLO W A; RAJAGOPALAN S; **VENKATESAN R**

Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5515307	A	19960507	US 94286161	A	19940804	199624	B

Priority Applications (No Type Date): US 94286161 A 19940804
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5515307	A		15	G06F-001/02	

Abstract (Basic): US 5515307 A

The method for generating an output stream of cryptographically strong pseudo-random bits from an input stream of either cryptographically strong pseudo-random bits or weakly random bits involves forming a matrix of bits from the input stream. A seed is formed from the input stream. A first set of bits is selected from the input stream, using the first set to select rows from the matrix and bitwise exclusive-OR'ing the selected rows to generate a matrix bit stream.

A second set of bits is selected from the input stream. The second set is used to generate a graph bit stream, the initial graph bit stream is obtained from a neighbour of the seed, with each subsequent graph bit stream being obtained from a neighbour of each previous graph bit stream. The output stream is generated as the bitwise exclusive-OR of the matrix bit stream and the graph bit stream.

USE/ADVANTAGE - Fast operation. Behaves almost as if it is using real random input and therefore ideal for simulators.

Dwg.2/5

Title Terms: STRONG; PSEUDO; RANDOM; BIT; GENERATE; PROPERTIES; RELATIVELY; SLOW; STRONG; GENERATOR; RAPID; MIX; PROPERTIES; RANDOM; WALKING; EXPAND; GRAPH
Derwent Class: T01; W01
International Patent Class (Main): **G06F-001/02**
International Patent Class (Additional): H04L-009/00
File Segment: EPI

6/5/36 (Item 36 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01397940
SYSTEM AND METHOD FOR INTERFACING A SOFTWARE PROCESS TO SECURE REPOSITORIES
SYSTEM UND VERFAHREN ZUR VERBINDUNG EINES SOFTWAREPROZESSES MIT SICHERHEITSVERZEICHNISSEN
SYST ME ET PROC D POUR INTERFACER UNE CONFIGURATION LOGICIELLE DESTIN E S CURISER DES ORGANES D'ARCHIVAGE

PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
MANFERDELLI, John, L., 7921 245th Way NE, Redmond, WA 98053, (US)
MARR, Michael, David, 21008 NE 36th Street, Sammamish, WA 98074, (US)
KRISHNASWAMY, Vinay, 23319 N.E. 142nd Pl., Woodinville, WA 98072, (US)
JAKUBOWSKI, Mariusz, H. , 1840 154th Avenue NE C-222, Bellevue, WA 98007 , (US

PATENT (CC, No, Kind, Date): WO 2002001334 020103
APPLICATION (CC, No, Date): EP 2001944670 010608; WO 2001US40899 010608
PRIORITY (CC, No, Date): US 604518 000627
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020227 A2 International application. (Art. 158(1))
Application: 020227 A2 International application entering European phase
Application: 030827 A2 International application. (Art. 158(1))
Appl Changed: 030827 A2 International application not entering European phase
Withdrawal: 030827 A2 Date application deemed withdrawn: 20030128
LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/37 (Item 37 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01397939
SYSTEM AND METHOD FOR PROVIDING AN INDIVIDUALIZED SECURE REPOSITORY
SYSTEM UND VERFAHREN ZUR ERZEUGUNG EINER INDIVIDIALISIERTEN SICHEREN DATENBANK
ORGANE D'ARCHIVAGE SUR PERSONNALISE, ET SYSTEME ET PROCEDE DE MISE EN OEUVRE DUDIT ORGANE D'ARCHIVAGE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
MANFERDELLI, John, L., 7921 245th Way NE, Redmond, WA 98053, (US)
MARR, Michael, David, 21008 NE 36th Street, Sammamish, WA 98074, (US)
KRISHNASWAMY, Vinay, 23319 NE 142nd Place, Woodinville, WA 98072, (US)
JAKUBOWSKI, Mariusz, H. , 1840 154th Avenue NE C-222, Bellevue, WA 98007 , (US
PATENT (CC, No, Kind, Date): WO 2002001333 020103
APPLICATION (CC, No, Date): EP 2001944669 010608; WO 2001US40898 010608
PRIORITY (CC, No, Date): US 604543 000627
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020227 A2 International application. (Art. 158(1))
Application: 020227 A2 International application entering European phase
Application: 030910 A2 International application. (Art. 158(1))
Appl Changed: 030910 A2 International application not entering European phase
Withdrawal: 030910 A2 Date application deemed withdrawn: 20030128
LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/38 (Item 38 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01397906
SECURE REPOSITORY WITH LAYERS OF TAMPER RESISTANCE AND SYSTEM AND METHOD FOR PROVIDING SAME
SICHERHEITSVERZEICHNIS MIT BETRUGSWIDERSTANDSSCHICHTEN UND SYSTEM UND VERFAHREN DAZU
REFERENTIEL SECURISE A COUCHES INFALSIFIABLES, ET SYSTEME ET PROCEDE UTILISANT LEDIT REFERENTIEL SECURISE
PATENT ASSIGNEE:

MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
MANFERDELLI, John, L., 7921 245th Way NE, Redmond, WA 98053, (US)
MARR, Michael, David, 21008 NE 36th Street, Sammamish, WA 98074, (US)
KRISHNASWAMY, Vinay, 23319 N.E. 142nd Pl., Woodinville, WA 98072, (US)
JAKUBOWSKI, Mariusz, H. , 1840 154th Avenue NE C-222, Bellevue, WA 98007 , (US
PATENT (CC, No, Kind, Date): WO 2002001327 020103
APPLICATION (CC, No, Date): EP 2001944393 010608; WO 2001US18670 010608
PRIORITY (CC, No, Date): US 604174 000627
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	020227	A2 International application. (Art. 158(1))
Application:	020227	A2 International application entering European phase
Application:	030827	A2 International application. (Art. 158(1))
Appl Changed:	030827	A2 International application not entering European phase
Withdrawal:	030827	A2 Date application deemed withdrawn: 20030128

LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/39 (Item 39 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01352772
TECHNIQUE FOR PRODUCING TAMPER-RESISTANT EXECUTABLE CODE THROUGH WATERMARKING
VERFAHREN ZUR ERZEUGUNG BETRUGSICHERER SOFTWARE DURCH WASSERZEICHEN
TECHNIQUE POUR PRODUIRE PAR APPLICATION DE FILIGRANE DU CODE EXECUTABLE A DEGRE D'INVIOLABILITE ELEVE ET CODE "MARQUE EN FILIGRANE" QUI EN RESULTE

PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington 98052-6399, (US), (Applicant designated States: all)
INVENTOR:
VENKATESAN, Ramarathnam , 17208 NE 22nd Ct., Redmond, WA 98052, (US)
VAZIRANI, Vijay, 801 Atlantic Aven., Georgia Inst. Techn. Comp., Atlanta, GA 30332, (US

PATENT (CC, No, Kind, Date): WO 2001069355 010920
APPLICATION (CC, No, Date): EP 2001907028 010207; WO 2001US3821 010207
PRIORITY (CC, No, Date): US 525694 000314
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 011114 A1 International application. (Art. 158(1))
Application: 011114 A1 International application entering European phase
Application: 030507 A1 International application. (Art. 158(1))
Appl Changed: 030507 A1 International application not entering European phase
Withdrawal: 030507 A1 Date application deemed withdrawn: 20021015
LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/40 (**Item** 40 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01352744
SECURE DISTRIBUTION OF DIGITAL PRODUCTS AGAINST UNAUTHORIZED USE
GESICHERTE VERTEILUNG VON DIGITALEN PRODUKTEN GEGEN UNBEFUGTEN GEBRAUCH
PROCEDES ET DISPOSITIFS DE CONFIGURATION ET DISTRIBUTION DE BIENS NUMERIQUES RESISTANTS AU PIRATAGE "BORE"

PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
PEINADO, Marcus, 7 168th Avenue NE, Bellevue, WA 98008, (US)
JAKUBOWSKI, Mariusz, H. , 1840 154th Avenue NE C-222, Bellevue, WA 98007, (US)
VENKATESAN, Ramarathnam , 17208 N.E. 22nd Ct., Redmond, WA 98052, (US

PATENT (CC, No, Kind, Date): WO 2001069354 010920
APPLICATION (CC, No, Date): EP 2001904905 010117; WO 2001US1609 010117
PRIORITY (CC, No, Date): US 525206 000314
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00**
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 011114 A2 International application. (Art. 158(1))
Application: 011114 A2 International application entering European phase
Application: 030507 A2 International application. (Art. 158(1))
Appl Changed: 030507 A2 International application not entering European phase
Withdrawal: 030507 A2 Date application deemed withdrawn: 20021015
LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/41 (Item 41 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01325573
PRODUCING A NEW BLACK BOX FOR A DIGITAL RIGHTS MANAGEMENT (DRM) SYSTEM
PRODUZIEREN EINER NEUEN BLACK BOX FUR EIN DIGITALES BERECHTIGUNGS-VERWALTUNGS-SYSTEM
PRODUCTION D'UNE NOUVELLE BOITE NOIRE POUR SYSTEME ELECTRONIQUE DE DROITS INTELLECTUELS
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
PEINADO, Marcus, 5007 148th NE, E207, Bellevue, WA 98007, (US)
VENKATESAN, Ramarathnam , 17208 NE 22nd Ct., Redmond, WA 98052, (US)
DAVIS, Malcolm, 10280 SE 6th Street 4, Bellevue, WA 98004, (US
PATENT (CC, No, Kind, Date): WO 2001052471 010719
APPLICATION (CC, No, Date): EP 2000957697 000822; WO 2000US23106 000822
PRIORITY (CC, No, Date): US 176425 P 000114; US 525509 000315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): H04L-009/08; **G06F-001/00**
CITED PATENTS (WO A): WO 9833106 A ; EP 679978 A ; EP 735719 A ; EP 387599 A ; US 5883955 A
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010912 A1 International application. (Art. 158(1))
Application: 010912 A1 International application entering European phase
Application: 030507 A1 International application. (Art. 158(1))
Appl Changed: 030507 A1 International application not entering European phase
Withdrawal: 030507 A1 Date application deemed withdrawn: 20020815
LANGUAGE (Publication,Procedural,Application): English; English; English

6/5/42 (Item 42 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01325572
ENCRYPTING A DIGITAL OBJECT BASED ON A KEY ID SELECTED THEREFOR
VERSCHLUSSELUNG EINES DIGITALEN OBJEKTS MIT EINER DAFUR AUSGEWAHLTEN SCHLUSSELIDENTIFIKATION
CHIFFREMENT D'UN OBJET NUMERIQUE A PARTIR D'UNE CLE ID SELECTIONNEE
PATENT ASSIGNEE:
MICROSOFT CORPORATION, (749866), One Microsoft Way, Redmond, WA 98052, (US), (Applicant designated States: all)
INVENTOR:
PEINADO, Marcus, 5007 - 148th Avenue NE, E207, Bellevue, WA 98007, (US)
VENKATESAN, Ramarathnam , 17208 NE 22nd Ct., Redmond, WA 98052, (US
PATENT (CC, No, Kind, Date): WO 2001052019 010719
APPLICATION (CC, No, Date): EP 2000957696 000822; WO 2000US23105 000822
PRIORITY (CC, No, Date): US 176425 P 000114; US 526292 000315
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS (V7): **G06F-001/00** ; H04L-009/08
CITED PATENTS (WO A): WO 9847259 A ; EP 768774 A ; US 5915025 A ; US 5999629 A ; EP 874300 A
LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010912 A1 International application. (Art. 158(1))
Application: 010912 A1 International application entering European phase
Application: 030312 A1 International application. (Art. 158(1))
Appl Changed: 030312 A1 International application not entering European phase
Withdrawal: 030312 A1 Date application deemed withdrawn: 20020815
LANGUAGE (Publication,Procedural,Application): English; English; English

Software Watermarking: Models and Dynamic Embeddings

Christian Collberg* Clark Thomborson

Department of Computer Science
The University of Auckland
Private Bag 92019
Auckland, New Zealand.
{collberg,cthombor}@cs.auckland.ac.nz

Abstract

Watermarking embeds a secret message into a cover message. In media watermarking the secret is usually a copyright notice and the cover a digital image. Watermarking an object discourages intellectual property theft, or when such theft has occurred, allows us to prove ownership.

The Software Watermarking problem can be described as follows. Embed a structure W into a program P such that: W can be reliably located and extracted from P even after P has been subjected to code transformations such as translation, optimization and obfuscation; W is stealthy; W has a high data rate; embedding W into P does not adversely affect the performance of P; and W has a mathematical property that allows us to argue that its presence in P is the result of deliberate actions.

In the first part of the paper we construct an informal taxonomy of software watermarking techniques. In the second part we formalize these results. Finally, we propose a new software watermarking technique in which a dynamic graphic watermark is stored in the execution state of a program.

1 Introduction

Apart from Grover [16] and a few recent US patents [10,21, 28,33], very little (publicly available) information seems to exist on *software watermarking* in which a copyright notice or customer identification number is embedded into a program. This is in contrast to media watermarking which is a very active area of research [4,6,22,30].

In the present paper we will try to bring together what little information does exist in the form of a taxonomy of software watermarking techniques, provide a formalization of software watermarking, and present new results on *dynamic data structure watermarking*.

*Author's present address: Department of Computer Science, University of Arizona, Tucson, AZ 85721. email: collberg@cs.arizona.edu

POPL 99 San Antonio Texas USA

1.1 Attacks on Watermarking Systems

The strength of any steganographic system is a function of its *data rate*, *stealth*, and *resilience*. The data rate expresses the quantity of hidden data that can be embedded within the cover message, the stealth expresses how imperceptible the embedded data is to an observer, and the resilience expresses the hidden message's degree of immunity to attack by an adversary. All steganographic systems exhibit a trade-off between these three metrics in that a high data rate implies low stealth and resilience. For example, the resilience of a watermark can easily be increased by exploiting redundancy (i.e. including it several times in the host message) but this will result in a reduction in bandwidth.

To evaluate the quality of a watermarking scheme we must also know how well it stands up to *different types* of attacks. In general, no steganographic scheme is immune to all attacks, and often several techniques have to be employed simultaneously to attain the required degree of resilience. In [6] Bender writes about media watermarking: "[] all of the proposed methods have limitations. The goal of achieving protection of large amounts of embedded data against intentional attempts at removal may be unobtainable."

To illustrate these concepts we will assume the following scenario. Alice watermarks a host object $\mathcal{O}$ with watermark $\mathcal{W}$ and key $\mathcal{K}$, and then sells $\mathcal{O}$ to Bob. Before Bob can sell $\mathcal{O}$ on to Douglas he must ensure that the watermark has been rendered useless, or else Alice will be able to prove that her intellectual property rights have been violated. Figure 1 shows the three principal kinds of attacks Bob can launch against the watermark:

subtractive attack If Bob can detect the presence and (approximate) location of $\mathcal{W}$, he may try to *crop* it out of $\mathcal{O}$. An *effective* subtractive attack is one where the cropped object has retained enough original content to still be of value to Bob.

distortive attack If Bob cannot locate $\mathcal{W}$ and is willing to accept some degradation in quality of $\mathcal{O}$, he can apply distortive transformations uniformly over the object and, hence, to any watermark it may contain. An *effective* distortive attack is one where Alice can no longer detect the degraded watermark, but the degraded object still has value to Bob.

additive attack Finally, Bob can augment $\mathcal{O}$ by inserting his own watermark $\mathcal{W}'$ (or several such marks). An *effective* additive attack is one in which Bob's mark completely overrides Alice's original mark so that it can no longer be extracted, or where it is impossible to detect that Alice's mark temporally precedes Bob's.